INSTALLATION AND OPERATION MANUAL

LA-210

EFM DSL Network Termination Unit

Version 1.5

CARRIER ETHERNET MEF Certified Compliant

EtherAccess

RAD data communications
The Access Company

LA-210

EFM DSL Network Termination Unit

Version 1.5

Installation and Operation Manual

Notice

This manual contains information that is proprietary to RAD Data Communications Ltd. ("RAD"). No part of this publication may be reproduced in any form whatsoever without prior written approval by RAD Data Communications.

Right, title and interest, all information, copyrights, patents, know-how, trade secrets and other intellectual property or other proprietary rights relating to this manual and to the LA-210 and any software components contained therein are proprietary products of RAD protected under international copyright law and shall be and remain solely with RAD.

LA-210 is a registered trademark of RAD. No right, license, or interest to such trademark is granted hereunder, and you agree that no such right, license, or interest shall be asserted by you with respect to such trademark.

You shall not copy, reverse compile or reverse assemble all or any portion of the Manual or the LA-210. You are prohibited from, and shall not, directly or indirectly, develop, market, distribute, license, or sell any product that supports substantially similar functionality as the LA-210, based on or derived in any way from the LA-210. Your undertaking in this paragraph shall survive the termination of this Agreement.

This Agreement is effective upon your opening of the LA-210 package and shall continue until terminated. RAD may terminate this Agreement upon the breach by you of any term hereof. Upon such termination by RAD, you agree to return to RAD the LA-210 and all copies and portions thereof.

For further information contact RAD at the address below or contact your local distributor.

International Headquarters
RAD Data Communications Ltd.

24 Raoul Wallenberg Street
Tel Aviv 69719, Israel
Tel: 972-3-6458181
Fax: 972-3-6498250, 6474436
E-mail: market@rad.com

North America Headquarters
RAD Data Communications Inc.

900 Corporate Drive
Mahwah, NJ 07430, USA
Tel: (201) 5291100, Toll free: 1-800-4447234
Fax: (201) 5295777
E-mail: market@radusa.com

© 1998–2007 RAD Data Communications Ltd. Publication No. 504-200-08/08

Limited Warranty

RAD warrants to DISTRIBUTOR that the hardware in the LA-210 to be delivered hereunder shall be free of defects in material and workmanship under normal use and service for a period of twelve (12) months following the date of shipment to DISTRIBUTOR.

If, during the warranty period, any component part of the equipment becomes defective by reason of material or workmanship, and DISTRIBUTOR immediately notifies RAD of such defect, RAD shall have the option to choose the appropriate corrective action: a) supply a replacement part, or b) request return of equipment to its plant for repair, or c) perform necessary repair at the equipment's location. In the event that RAD requests the return of equipment, each party shall pay one-way shipping costs.

RAD shall be released from all obligations under its warranty in the event that the equipment has been subjected to misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than RAD's own authorized service personnel, unless such repairs by others were made with the written consent of RAD.

The above warranty is in lieu of all other warranties, expressed or implied. There are no warranties which extend beyond the face hereof, including, but not limited to, warranties of merchantability and fitness for a particular purpose, and in no event shall RAD be liable for consequential damages.

RAD shall not be liable to any person for any special or indirect damages, including, but not limited to, lost profits from any cause whatsoever arising from or in any way connected with the manufacture, sale, handling, repair, maintenance or use of the LA-210, and in no event shall RAD's liability exceed the purchase price of the LA-210.

DISTRIBUTOR shall be responsible to its customers for any and all warranties which it makes relating to LA-210 and for ensuring that replacements and other adjustments required in connection with the said warranties are satisfactory.

Software components in the LA-210 are provided "as is" and without warranty of any kind. RAD disclaims all warranties including the implied warranties of merchantability and fitness for a particular purpose. RAD shall not be liable for any loss of use, interruption of business or indirect, special, incidental or consequential damages of any kind. In spite of the above RAD shall do its best to provide error-free software products and shall offer free Software updates during the warranty period under this Agreement.

RAD's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement and the LA-210 shall not exceed the sum paid to RAD for the purchase of the LA-210. In no event shall RAD be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if RAD has been advised of the possibility of such damages.

This Agreement shall be construed and governed in accordance with the laws of the State of Israel.

Product Disposal

To facilitate the reuse, recycling and other forms of recovery of waste equipment in protecting the environment, the owner of this RAD product is required to refrain from disposing of this product as unsorted municipal waste at the end of its life cycle. Upon termination of the unit's use, customers should provide for its collection for reuse, recycling or other form of environmentally conscientious disposal.

General Safety Instructions

The following instructions serve as a general guide for the safe installation and operation of telecommunications products. Additional instructions, if applicable, are included inside the manual.

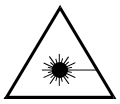
Safety Symbols

Warning

This symbol may appear on the equipment or in the text. It indicates potential safety hazards regarding product operation or maintenance to operator or service personnel.

Danger of electric shock! Avoid any contact with the marked surface while the product is energized or connected to outdoor telecommunication lines.

Protective ground: the marked lug or terminal should be connected to the building protective ground bus.



Warning

Some products may be equipped with a laser diode. In such cases, a label with the laser class and other warnings as applicable will be attached near the optical transmitter. The laser warning symbol may be also attached.

Please observe the following precautions:

- Before turning on the equipment, make sure that the fiber optic cable is intact and is connected to the transmitter.
- Do not attempt to adjust the laser drive current.
- Do not use broken or unterminated fiber-optic cables/connectors or look straight at the laser beam.
- The use of optical devices with the equipment will increase eye hazard.
- Use of controls, adjustments or performing procedures other than those specified herein, may result in hazardous radiation exposure.

ATTENTION: The laser beam may be invisible!

In some cases, the users may insert their own SFP laser transceivers into the product. Users are alerted that RAD cannot be held responsible for any damage that may result if non-compliant transceivers are used. In particular, users are warned to use only agency approved products that comply with the local laser safety regulations for Class 1 laser products.

Always observe standard safety precautions during installation, operation and maintenance of this product. Only qualified and authorized service personnel should carry out adjustment, maintenance or repairs to this product. No installation, adjustment, maintenance or repairs should be performed by either the operator or the user.

Handling Energized Products

General Safety Practices

Do not touch or tamper with the power supply when the power cord is connected. Line voltages may be present inside certain products even when the power switch (if installed) is in the OFF position or a fuse is blown. For DC-powered products, although the voltages levels are usually not hazardous, energy hazards may still exist.

Before working on equipment connected to power lines or telecommunication lines, remove jewelry or any other metallic object that may come into contact with energized parts.

Unless otherwise specified, all products are intended to be grounded during normal use. Grounding is provided by connecting the mains plug to a wall socket with a protective ground terminal. If a ground lug is provided on the product, it should be connected to the protective ground at all times, by a wire with a diameter of 18 AWG or wider. Rack-mounted equipment should be mounted only in grounded racks and cabinets.

Always make the ground connection first and disconnect it last. Do not connect telecommunication cables to ungrounded equipment. Make sure that all other cables are disconnected before disconnecting the ground.

Connecting AC Mains

Make sure that the electrical installation complies with local codes.

Always connect the AC plug to a wall socket with a protective ground.

The maximum permissible current capability of the branch distribution circuit that supplies power to the product is 16A. The circuit breaker in the building installation should have high breaking capacity and must operate at short-circuit current exceeding 35A.

Always connect the power cord first to the equipment and then to the wall socket. If a power switch is provided in the equipment, set it to the OFF position. If the power cord cannot be readily disconnected in case of emergency, make sure that a readily accessible circuit breaker or emergency switch is installed in the building installation.

In cases when the power distribution system is IT type, the switch must disconnect both poles simultaneously.

Connecting DC Power

Unless otherwise specified in the manual, the DC input to the equipment is floating in reference to the ground. Any single pole can be externally grounded.

Due to the high current capability of DC power systems, care should be taken when connecting the DC supply to avoid short-circuits and fire hazards.

DC units should be installed in a restricted access area, i.e. an area where access is authorized only to qualified service and maintenance personnel.

Make sure that the DC power supply is electrically isolated from any AC source and that the installation complies with the local codes.

The maximum permissible current capability of the branch distribution circuit that supplies power to the product is 16A. The circuit breaker in the building installation should have high breaking capacity and must operate at short-circuit current exceeding 35A.

Before connecting the DC supply wires, ensure that power is removed from the DC circuit. Locate the circuit breaker of the panel board that services the equipment and switch it to the OFF position. When connecting the DC supply wires, first connect the ground wire to the corresponding terminal, then the positive pole and last the negative pole. Switch the circuit breaker back to the ON position.

A readily accessible disconnect device that is suitably rated and approved should be incorporated in the building installation.

If the DC power supply is floating, the switch must disconnect both poles simultaneously.

Connecting Data and Telecommunications Cables

Data and telecommunication interfaces are classified according to their safety status.

The following table lists the status of several standard interfaces. If the status of a given port differs from the standard one, a notice will be given in the manual.

Ports	**Safety Status**	
V.11, V.28, V.35, V.36, RS-530, X.21, 10 BaseT, 100 BaseT, Unbalanced E1, E2, E3, STM, DS-2, DS-3, S-Interface ISDN, Analog voice E&M	SELV	Safety Extra Low Voltage: Ports which do not present a safety hazard. Usually up to 30 VAC or 60 VDC.
xDSL (without feeding voltage), Balanced E1, T1, Sub E1/T1	TNV-1	Telecommunication Network Voltage-1: Ports whose normal operating voltage is within the limits of SELV, on which overvoltages from telecommunications networks are possible.
FXS (Foreign Exchange Subscriber)	TNV-2	Telecommunication Network Voltage-2: Ports whose normal operating voltage exceeds the limits of SELV (usually up to 120 VDC or telephone ringing voltages), on which overvoltages from telecommunication networks are not possible. These ports are not permitted to be directly connected to external telephone and data lines.
FXO (Foreign Exchange Office), xDSL (with feeding voltage), U-Interface ISDN	TNV-3	Telecommunication Network Voltage-3: Ports whose normal operating voltage exceeds the limits of SELV (usually up to 120 VDC or telephone ringing voltages), on which overvoltages from telecommunication networks are possible.

Always connect a given port to a port of the same safety status. If in doubt, seek the assistance of a qualified safety engineer.

Always make sure that the equipment is grounded before connecting telecommunication cables. Do not disconnect the ground connection before disconnecting all telecommunications cables.

Some SELV and non-SELV circuits use the same connectors. Use caution when connecting cables. Extra caution should be exercised during thunderstorms.

When using shielded or coaxial cables, verify that there is a good ground connection at both ends. The grounding and bonding of the ground connections should comply with the local codes.

The telecommunication wiring in the building may be damaged or present a fire hazard in case of contact between exposed external wires and the AC power lines. In order to reduce the risk,

there are restrictions on the diameter of wires in the telecom cables, between the equipment and the mating connectors.

Caution To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cords.

Attention Pour réduire les risques s'incendie, utiliser seulement des conducteurs de télécommunications 26 AWG ou de section supérieure.

Some ports are suitable for connection to intra-building or non-exposed wiring or cabling only. In such cases, a notice will be given in the installation instructions.

Do not attempt to tamper with any carrier-provided equipment or connection hardware.

Electromagnetic Compatibility (EMC)

The equipment is designed and approved to comply with the electromagnetic regulations of major regulatory bodies. The following instructions may enhance the performance of the equipment and will provide better protection against excessive emission and better immunity against disturbances.

A good ground connection is essential. When installing the equipment in a rack, make sure to remove all traces of paint from the mounting points. Use suitable lock-washers and torque. If an external grounding lug is provided, connect it to the ground bus using braided wire as short as possible.

The equipment is designed to comply with EMC requirements when connecting it with unshielded twisted pair (UTP) cables. However, the use of shielded wires is always recommended, especially for high-rate data. In some cases, when unshielded wires are used, ferrite cores should be installed on certain cables. In such cases, special instructions are provided in the manual.

Disconnect all wires which are not in permanent use, such as cables used for one-time configuration.

The compliance of the equipment with the regulations for conducted emission on the data lines is dependent on the cable quality. The emission is tested for UTP with 80 dB longitudinal conversion loss (LCL).

Unless otherwise specified or described in the manual, TNV-1 and TNV-3 ports provide secondary protection against surges on the data lines. Primary protectors should be provided in the building installation.

The equipment is designed to provide adequate protection against electro-static discharge (ESD). However, it is good working practice to use caution when connecting cables terminated with plastic connectors (without a grounded metal hood, such as flat cables) to sensitive data lines. Before connecting such cables, discharge yourself by touching ground or wear an ESD preventive wrist strap.

FCC-15 User Information

This equipment has been tested and found to comply with the limits of the Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the Installation and Operation manual, may cause harmful interference to the radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Emission Requirements

This Class A digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulation.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Warning per EN 55022 (CISPR-22)

Warning	This is a class A product. In a domestic environment, this product may cause radio interference, in which case the user will be required to take adequate measures.
Avertissement	Cet appareil est un appareil de Classe A. Dans un environnement résidentiel, cet appareil peut provoquer des brouillages radioélectriques. Dans ces cas, il peut être demandé à l'utilisateur de prendre les mesures appropriées.
Achtung	Das vorliegende Gerät fällt unter die Funkstörgrenzwertklasse A. In Wohngebieten können beim Betrieb dieses Gerätes Rundfunkströrungen auftreten, für deren Behebung der Benutzer verantwortlich ist.

Mise au rebut du produit

Afin de faciliter la réutilisation, le recyclage ainsi que d'autres formes de récupération d'équipement mis au rebut dans le cadre de la protection de l'environnement, il est demandé au propriétaire de ce produit RAD de ne pas mettre ce dernier au rebut en tant que déchet municipal non trié, une fois que le produit est arrivé en fin de cycle de vie. Le client devrait proposer des solutions de réutilisation, de recyclage ou toute autre forme de mise au rebut de cette unité dans un esprit de protection de l'environnement, lorsqu'il aura fini de l'utiliser.

Instructions générales de sécurité

Les instructions suivantes servent de guide général d'installation et d'opération sécurisées des produits de télécommunications. Des instructions supplémentaires sont éventuellement indiquées dans le manuel.

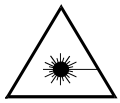
Symboles de sécurité

Avertissement

Ce symbole peut apparaitre sur l'équipement ou dans le texte. Il indique des risques potentiels de sécurité pour l'opérateur ou le personnel de service, quant à l'opération du produit ou à sa maintenance.

Danger de choc électrique ! Evitez tout contact avec la surface marquée tant que le produit est sous tension ou connecté à des lignes externes de télécommunications.

Mise à la terre de protection : la cosse ou la borne marquée devrait être connectée à la prise de terre de protection du bâtiment.



Avertissement

Certains produits peuvent être équipés d'une diode laser. Dans de tels cas, une étiquette indiquant la classe laser ainsi que d'autres avertissements, le cas échéant, sera jointe près du transmetteur optique. Le symbole d'avertissement laser peut aussi être joint.

Veuillez observer les précautions suivantes :

- Avant la mise en marche de l'équipement, assurez-vous que le câble de fibre optique est intact et qu'il est connecté au transmetteur.
- Ne tentez pas d'ajuster le courant de la commande laser.
- N'utilisez pas des câbles ou connecteurs de fibre optique cassés ou sans terminaison et n'observez pas directement un rayon laser.
- L'usage de périphériques optiques avec l'équipement augmentera le risque pour les yeux.
- L'usage de contrôles, ajustages ou procédures autres que celles spécifiées ici pourrait résulter en une dangereuse exposition aux radiations.

ATTENTION : Le rayon laser peut être invisible !

Les utilisateurs pourront, dans certains cas, insérer leurs propres émetteurs-récepteurs Laser SFP dans le produit. Les utilisateurs sont avertis que RAD ne pourra pas être tenue responsable de tout dommage pouvant résulter de l'utilisation d'émetteurs-récepteurs non conformes. Plus particulièrement, les utilisateurs sont avertis de n'utiliser que des produits approuvés par l'agence et conformes à la réglementation locale de sécurité laser pour les produits laser de classe 1.

Respectez toujours les précautions standards de sécurité durant l'installation, l'opération et la maintenance de ce produit. Seul le personnel de service qualifié et autorisé devrait effectuer l'ajustage, la maintenance ou les réparations de ce produit. Aucune opération d'installation, d'ajustage, de maintenance ou de réparation ne devrait être effectuée par l'opérateur ou l'utilisateur.

Manipuler des produits sous tension

Règles générales de sécurité

Ne pas toucher ou altérer l'alimentation en courant lorsque le câble d'alimentation est branché. Des tensions de lignes peuvent être présentes dans certains produits, même lorsque le commutateur (s'il est installé) est en position OFF ou si le fusible est rompu. Pour les produits alimentés par CC, les niveaux de tension ne sont généralement pas dangereux mais des risques de courant peuvent toujours exister.

Avant de travailler sur un équipement connecté aux lignes de tension ou de télécommunications, retirez vos bijoux ou tout autre objet métallique pouvant venir en contact avec les pièces sous tension.

Sauf s'il en est autrement indiqué, tous les produits sont destinés à être mis à la terre durant l'usage normal. La mise à la terre est fournie par la connexion de la fiche principale à une prise murale équipée d'une borne protectrice de mise à la terre. Si une cosse de mise à la terre est fournie avec le produit, elle devrait être connectée à tout moment à une mise à la terre de protection par un conducteur de diamètre 18 AWG ou plus. L'équipement monté en châssis ne devrait être monté que sur des châssis et dans des armoires mises à la terre.

Branchez toujours la mise à la terre en premier et débranchez-la en dernier. Ne branchez pas des câbles de télécommunications à un équipement qui n'est pas mis à la terre. Assurez-vous que tous les autres câbles sont débranchés avant de déconnecter la mise à la terre.

Connexion au courant du secteur

Assurez-vous que l'installation électrique est conforme à la réglementation locale.

Branchez toujours la fiche de secteur à une prise murale équipée d'une borne protectrice de mise à la terre.

La capacité maximale permissible en courant du circuit de distribution de la connexion alimentant le produit est de 16A. Le coupe-circuit dans l'installation du bâtiment devrait avoir une capacité élevée de rupture et devrait fonctionner sur courant de court-circuit dépassant 35A.

Branchez toujours le câble d'alimentation en premier à l'équipement puis à la prise murale. Si un commutateur est fourni avec l'équipement, fixez-le en position OFF. Si le câble d'alimentation ne peut pas être facilement débranché en cas d'urgence, assurez-vous qu'un coupe-circuit ou un disjoncteur d'urgence facilement accessible est installé dans l'installation du bâtiment.

Le disjoncteur devrait déconnecter simultanément les deux pôles si le système de distribution de courant est de type IT.

Connexion d'alimentation CC

Sauf s'il en est autrement spécifié dans le manuel, l'entrée CC de l'équipement est flottante par rapport à la mise à la terre. Tout pôle doit être mis à la terre en externe.

A cause de la capacité de courant des systèmes à alimentation CC, des précautions devraient être prises lors de la connexion de l'alimentation CC pour éviter des courts-circuits et des risques d'incendie.

Les unités CC devraient être installées dans une zone à accès restreint, une zone où l'accès n'est autorisé qu'au personnel qualifié de service et de maintenance.

Assurez-vous que l'alimentation CC est isolée de toute source de courant CA (secteur) et que l'installation est conforme à la réglementation locale.

La capacité maximale permissible en courant du circuit de distribution de la connexion alimentant le produit est de 16A. Le coupe-circuit dans l'installation du bâtiment devrait avoir une capacité élevée de rupture et devrait fonctionner sur courant de court-circuit dépassant 35A.

Avant la connexion des câbles d'alimentation en courant CC, assurez-vous que le circuit CC n'est pas sous tension. Localisez le coupe-circuit dans le tableau desservant l'équipement et fixez-le en position OFF. Lors de la connexion de câbles d'alimentation CC, connectez d'abord le conducteur de mise à la terre à la borne correspondante, puis le pôle positif et en dernier, le pôle négatif. Remettez le coupe-circuit en position ON.

Un disjoncteur facilement accessible, adapté et approuvé devrait être intégré à l'installation du bâtiment.

Le disjoncteur devrait déconnecter simultanément les deux pôles si l'alimentation en courant CC est flottante.

Declaration of Conformity

Manufacturer's Name:	RAD Data Communications Ltd.
Manufacturer's Address:	24 Raoul Wallenberg St. Tel Aviv 69719 Israel

Declares that the product:

Product Name:	**LA-210**

Conforms to the following standard(s) or other normative document(s):

EMC	EN 55022:2006	Information technology equipment - Radio disturbance characteristics – Limits and methods of measurement.
	EN 55024:1998 + A1:2001, A2:2003	Information technology equipment - Immunity characteristics - Limits and methods of measurement.
	EN 61000-3-2:2000 + A2:2005	Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions (equipment input current up to and including 16A per phase).
	EN 61000-3-3:1995 + A1:2001	Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems, for equipment with rated current≤16A per phase and not subject to conditional connection.
Safety	EN 60950-1:2001 + A11:2004	Information technology equipment - Safety - Part 1: General requirements.

Supplementary **Information**:

The product herewith complies with the requirements of the EMC Directive 2004/108/EC, the Low Voltage Directive 2006/95/EC and the R&TTE Directive 99/5/EC for wired equipment. The product was tested in a typical configuration.

Tel Aviv, 24 August 2008

Haim Karshen

VP Quality

European Contact: RAD Data Communications GmbH
Otto-Hahn-Str. 28-30, 85521 Ottobrunn-Riemerling, Germany

Glossary

Address	A coded representation of the origin or destination of data.
Analog	A continuous wave or signal (such as human voice).
AWG	The American Wire Gauge System, which specifies wire width.
Balanced	A transmission line in which voltages on the two conductors are equal in magnitude, but opposite in polarity, with respect to ground.
Bus	A transmission path or channel. A bus is typically an electrical connection with one or more conductors, where all attached devices receive all transmissions at the same time.
Carrier	A continuous signal at a fixed frequency that is capable of being modulated with a second (information carrying) signal.
Channel	A path for electrical transmission between two or more points. Also called a link, line, circuit or facility.
Data	Information represented in digital form, including voice, text, facsimile and video.
Digital	The binary ("1" or "0") output of a computer or terminal. In data communications, an alternating, non-continuous (pulsating) signal.
DSL (Digital Subscriber Line)	A family of technologies for bringing broadband information (data and voice) to residential and business customers over the copper wires of a local telephone network. DSL technology provides extended range digital data transmission. Data rates (download and upload speeds) vary according to the distance from the central office, DSL technology, line conditions, and the service level implemented. Common DSL technologies include ADSL, VDSL, SHDSL, and G.SHDSL.bis.
E3	The European standard for high speed digital transmission, operating at 34 Mbps.
Flow Control	A congestion control mechanism that results in an ATM system implementing flow control.
FXO (Foreign Exchange Office)	A voice interface, emulating a PBX extension, as it appears to the CO (Central Office) for connecting a PBX extension to a multiplexer.
FXS (Foreign Exchange Subscriber)	A voice interface, emulating the extension interface of a PBX (or subscriber interface of a CO) for connecting a regular telephone set to a multiplexer.
Interface	A shared boundary, defined by common physical interconnection characteristics, signal characteristics, and meanings of exchanged

	signals.
Laser	A device that transmits an extremely narrow and coherent beam of electromagnetic energy in the visible light spectrum. Used as a light source for fiber optic transmission (generally more expensive, shorter lived, single mode only, for greater distances than LED).
Multiplexer	At one end of a communications link, a device that combines several lower speed transmission channels into a single high speed channel. A multiplexer at the other end reverses the process. Sometimes called a mux. See **Bit Interleaving/Multiplexing**.
Network	(1) An interconnected group of nodes. (2) A series of points, nodes, or stations connected by communications channels; the collection of equipment through which connections are made between data stations.
Port	The physical interface to a computer or multiplexer, for connection of terminals and modems.
Single Mode	Describing an optical wave-guide or fiber that is designed to propagate light of only a single wavelength (typically 5-10 microns in diameter).
T1	A digital transmission link with a capacity of 1.544 Mbps used in North America. Typically channelized into 24 DS0s, each capable of carrying a single voice conversation or data stream. Uses two pairs of twisted pair wires.

Quick Start Guide

LA-210 should be installed by an experienced technician only. If you are familiar with LA-210, use this guide to prepare the unit for operation.

1. Installing LA-210

Connecting the Interfaces

➤ To connect the interfaces:

1. Connect the SHDSL line to the RJ-45 connector designated SHDSL.
2. Connect the user LAN to the RJ-45 connector designated 10/100BaseT (up to four connectors).
3. Connect the control terminal to the front panel CONTROL connector.

   or

   Connect a Telnet host, a PC running a Web browsing application (ConfiguRAD), or an SNMP management station to the Ethernet port.

Connecting the Power

➤ To connect the power:

- Connect the power cable to the power socket on the LA-210 rear panel and the other end to the power outlet.

  The unit has no power switch. Operation starts when the power is applied to the power connector.

2. Configuring LA-210

Configure LA-210 to the desired operation mode via an ASCII terminal connected to the rear panel CONTROL port. After configuring, you can manage the unit over Telnet, a PC running a Web browsing application (ConfiguRAD) or SNMP via the Ethernet port or inband.

Note *Remote management requires assigning a host IP address.*

Starting a Terminal Session

➤ To start a terminal session:

1. Turn on the control terminal PC and set its default port parameters to 9.6 kbps, 8 bits/character, 1 stop bit, no parity.
2. Set the terminal emulator to ANSI VT100 emulation (for optimal view of system menus).
3. Set the terminal screen to show 132 characters.
4. Enter your user name and password and proceed with the management session.

Note *The default user name is* ***su****, and the default password is* ***1234****.*

Configuring LA-210 for Management

In order to establish a proper link with a network management station, it is necessary to assign an IP address to the LA-210 host and add the NMS to the manager list.

➤ To assign an IP address to the LA-210 host:

- In the Host menu (Configuration › System › Management › Host), assign an IP address to the LA-210 host.

➤ To configure the manager IP addresses:

- In the Manager List menu (Configuration › System › Management › Managers List), enter the manager IP address(es).

Configuring the Internal Bridge

This section instructs you on operating LA-210 in Bridge mode.

The internal bridge parameters, as well as the bridge ports and the VLAN membership must be configured according to the application requirements.

➤ To configure the internal bridge:

- In the Bridge menu (Configuration › Applications › Bridge), configure the VLAN and filtering modes of the LA-210 bridge.

➤ To configure the bridge ports:

- From the Bridge Port menu (Configuration› Applications › Bridge › Bridge Port), select a bridge port and configure the necessary parameters.

➤ To configure the VLAN membership:

- In the VLAN Membership menu (Configuration › Applications › Bridge › VLAN Membership), create a new VLAN and define the egress tagged and untagged ports which are the VLAN members.

Configuring the QoS

In order to prioritize the traffic, you have to choose a priority classification method and assign priorities to the traffic queues according to the selected method.

➤ **To set LA-210 to the Bridge mode (default settings):**

- In the System menu (Configuration › System), select **Application Mode** and then select **Save**.

  LA-210 is set to the Bridge mode if it was previously in Flow mode.

➤ **To configure the priority classification method:**

- From the QoS (Configuration › Applications › QoS) menu, select **Priority Classification** and choose the desired traffic classification method: 802.1p, DSCP or Per Port.

➤ **To assign priorities to the traffic queues:**

- In the Priority Mapping menu (Configuration › Applications › QoS › Priority Mapping), assign priorities to the traffic queues according to the selected method.

Configuring the Flows

This section instructs you on switching LA-210 to Flows mode and accessing the Flows menus.

➤ **To set LA-210 to the Flows mode:**

- In the System menu (Configuration › System), select **Application Mode** and then select **Save**.

  LA-210 is set to the Flows mode if it was previously in Bridge mode.

➤ **To configure the flows:**

1. Navigate to the Flows menu (Configuration › Applications › Flows).

   The menus for the Flow interfaces and the Flow definitions are available.

2. Define the flow interfaces and set up the flow definitions.

Contents

Chapter 1. Introduction

1.1 Overview....1-1
Product Options....1-1
Applications....1-2
Main Features....1-2
1.2 Physical Description....1-6
1.3 Functional Description....1-7
Interfaces....1-7
Ethernet Access (Bridge Mode)....1-7
Ethernet Access (Flow Mode)....1-12
Quality of Service....1-13
Management....1-14
Statistics....1-15
Event Log File....1-15
Diagnostics and Troubleshooting....1-15
1.4 Technical Specifications....1-16

Chapter 2. Installation and Setup

2.1 Site Requirements and Prerequisites....2-1
2.2 Package Contents....2-2
2.3 Required Equipment....2-2
Hand Tools and Kits....2-2
Power Cable....2-2
Cable and Connectors....2-2
2.4 Mounting the Unit....2-3
2.5 Connecting to SHDSL Equipment....2-3
2.6 Connecting to the Ethernet Equipment....2-3
2.7 Connecting to the ASCII Terminal....2-4
2.8 Connecting to Power....2-5
Connecting AC Power....2-5
Connecting DC Power....2-5

Chapter 3. Operation

3.1 Turning On the Unit....3-1
3.2 Indicators....3-1
3.3 Default Settings....3-2
3.4 Configuration and Management Alternatives....3-9
Working with Terminal....3-9
Working with ConfiguRAD....3-13
3.5 Turning Off the Unit....3-17

Chapter 4. Configuration

4.1 Configuring for Management....4-1
Entering Device Information....4-1
Configuring IP Host Parameters....4-2
Selecting the Terminal Baud Rate....4-3
Configuring Management Access....4-4

4.2 Configuring for Operation 4-10
Setting System Level Parameters 4-10
Configuring Physical Layer Port Parameters 4-13
Configuring the Application Layer Parameters 4-17
4.3 Additional Tasks 4-45
Displaying the Inventory 4-45
Changing User Name and Password 4-46
Transferring Software and Configuration Files 4-48
Resetting LA-210 4-49

Chapter 5. Configuring a Flow-Based Point-To-Point Application

5.1 Assembling the Hardware 5-1
Required Equipment 5-1
Connecting Cables 5-1
5.2 Configuring the Units for Basic Applications 5-2
Configuration Overview 5-2
Accessing ETX-202 and LA-210 Units 5-3
Configuring LA-210 5-4
Configuring ETX-202 Server and Client 5-7
5.3 Configuring the Units for Advanced Configurations 5-9
Configuring the DSLAM 5-17
5.4 Using the Setup to Screen a Movie 5-18
Using the VLC Media Player 5-18
5.5 Testing the Flow Based Configuration 5-19
Ping Tests 5-19
Policer Testing 5-20
Priority Testing 5-26

Chapter 6. Diagnostics and Troubleshooting

6.1 Monitoring Performance 6-1
Displaying System Status Informathion 6-1
Displaying the Physical Port Status 6-3
Displaying Application-Level Status 6-6
6.2 Displaying Statistics 6-8
Displaying Ethernet Port Statistics 6-8
Clearing Ethernet Port Statistics 6-9
Displaying SHDSL Port Statistics 6-10
Clearing the SHDSL Port Statistics 6-15
Displaying Flow Statistics 6-16
Displaying End-to-End Statistics for OAM 6-17
Viewing Radius Statistics 6-20
6.3 Handling Alarms and Traps 6-21
Displaying the Event Log File 6-21
Clearing the Event Log File 6-23
6.4 Troubleshooting 6-24
6.5 Testing the Unit 6-24
Running a Ping Test 6-24
Tracing the Route 6-25
OAM Tests 6-26
6.6 Technical Support 6-28

Appendix A. Pinouts
Appendix B. Boot Manager

Chapter 1
Introduction

1.1 Overview

LA-210 is an enhanced Ethernet Access Device, MEF 9 and MEF 14 certified for EPL (Ethernet Private Line) and EVPL (Ethernet Virtual Private Line) services. Operating in both Bridge and Flow based working modes, incoming customer traffic is classified and mapped according to port-based (all-in-one) bundling or by user port and CE VLAN-ID, VLAN priority, DSCP and IP precedence. This offers operators the flexibility to differentiate services using different kinds of classification methods, police this traffic and enforce SLA per service.

Operating at rates of up to 22 Mbps using G.SHDSL.bis EFM bonding technology enables transmitting data rates of up to 5.7 Mbps over each copper pair with EFM bonding (2-wire line).

LA-210 supports multiple data rates and works in full duplex mode over 2-wire, 4-wire, or 8-wire lines.

In addition to the EFM mode, LA-210 operates the SHDSL link in ATM mode to be compatible with the existing DSLAM infrastructure.

End-to-end OAM, based on IEEE 802.1ag and ITU-T Y.1731 enables Ethernet service providers to monitor their services proactively, measure end-to-end performance and guarantee that the customers receive the contracted SLA. Fault monitoring and performance measurement include Frame Delay, Frame Delay Variation, Frame Loss and Availability. LA-210 support also Single segment (link) OAM according to IEEE 802.3ah fault indication, including remote loopback.

Product Options

Line Interface

LA-210 supports G.SHDSL.bis twisted pair wire-line connections and can be ordered with one of the following wire pairs:

- One pair (2-wire)
- Two pairs (4-wire)
- Four pairs (8-wire).

Unit Enclosure

LA-210 ships with a plastic enclosure.

Applications

LA-210 is a suitable match for corporate, small-medium enterprise and SOHO customers, which require robust and secure connectivity using Layer 2 VPN or LAN connectivity. LA-210 is designed to meet those requirements by utilizing MEF-defined applications:

- Ethernet Private Line (EPL) – site-to-site connectivity over dedicated bandwidth without service multiplexing (see *Figure 1-1*)
- Ethernet Virtual Private Line (EVPL) – site-to-site connectivity over shared bandwidth with service multiplexing (see *Figure 1-2*).

Figure 1-1. Connecting LANs via Ethernet Private Line (EPL)

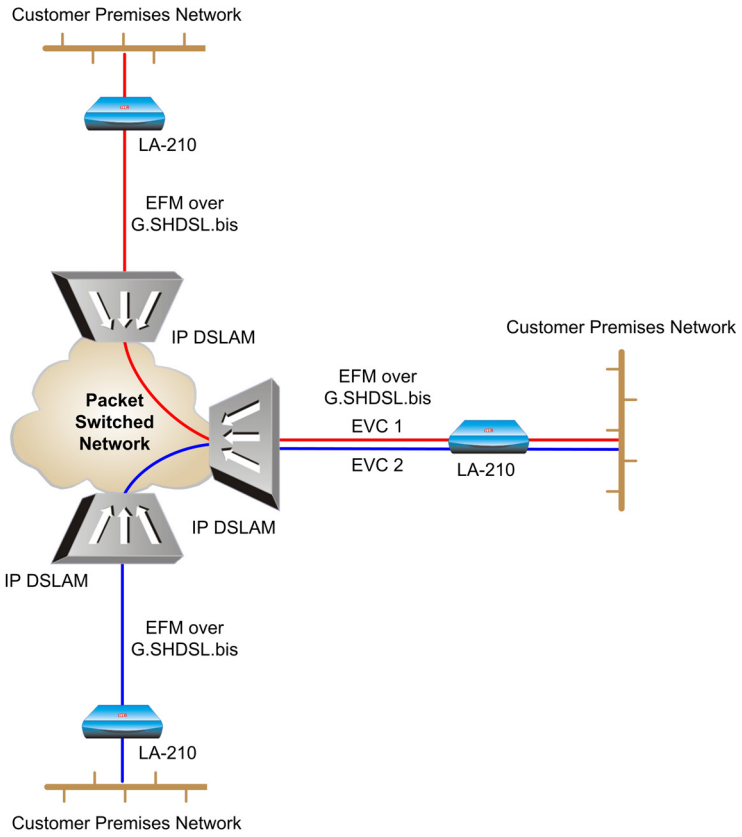


Figure 1-2. Providing L2 VPN using Ethernet Virtual Private Line (EVPL) Service

Main Features

This section lists the main features of LA-210.

Ethernet Interfaces

LA-210 provides one or four half-/full-duplex, 10/100 Mbps Fast Ethernet ports, with flow control and autonegotiation support. All ports are used for user traffic.

SHDSL Network Interfaces

LA-210 supports the following features per SHDSL line:

- Enhanced SHDSL ITU-T G.991.2 recommendation for user data rates n × 64 kbps (n = 1..89) up to 5696 kpbs
- Uses TC-PAM 16 or TC-PAM 32 to support higher data rates for G.991.2 Annexes F and G
- SHDSL twisted pair wire-line connection with one pair (2-wires), two pairs (4-wires), or four pairs (8-wires) of wires
- The line rate can be configured to adapt to the line condition (noise, loop attenuation, and so on) or set to a fixed rate
- Embedded Operations Channel (EOC) according to G.991.2 recommendation.
- Typical ranges (26 AWG, noise-free) are:

Table 1-1. Typical ranges (26 AWG)

Data Rate	2-wire		4-wire		4x2-wire	
[kbps]	[km]	[mi]	[km]	[mi]	[km]	[mi]
192	8	4.9	8	4.9	8	4.9
512	6.4	3.9	6.7	4.1	6.7	4.1
1536	5.7	3.5	6	3.7	6.5	4
2048	5.1	3.1	5.7	3.5	6.4	3.9
4096	3.9	2.4	5.1	3.1	5.7	3.5
4608	3.5	2.1	5	3	5.5	3.4
5696	2.9	1.8	4.6	2.8	5.1	3.1
11392	--	--	2.9	1.8	4.6	2.8
17088	--	--	--	--	3.5	2.1
22784	--	--	--	--	2.9	1.8

Operational Mode

LA-210 can operate in Bridge or Flow mode, which can be configured by the user. The internal bridge operates in VLAN aware and VLAN unaware modes.

Bridge Mode

In VLAN mode, VLAN stacking can be used for traffic separation between different users or services, by defining a Service VLAN ID per customer or service. When VLAN stacking is used, a Service VLAN tag is added to the user traffic and removed from network traffic. Both Service VLAN ID and Service VLAN priority can be defined.

Flow Mode

Incoming customer traffic is mapped to the Ethernet flows according to user defined per-port criteria.

Main flow mode features are:

- MEF 9 and 14 certified.
- Up to 8 flows are supported
    - Flow and Flow.CoS support.
- EPL services supported.
- EVPL services supported
- Two rate three color policer at Flow or Flow.CoS level
- VLAN manipulation (stacking) at port egress
- P bit marking
- Priority mapping to egress queues according 802.1p, DHCP or IP precedence.

Traffic Prioritization

LA-210 supports enhanced traffic prioritization and QoS to ensure service level agreements (SLA) that comply with business customer's high demands.

In Flow mode, traffic policing is applied per service and operates according to the dual leaky bucket mechanism based on CIR + CBS and EIR + EBS. User traffic is mapped into up to four separate queues, which can be configured to work as strict priority or weighted fair queue (WFQ).

The queues handle traffic with different service demands, such as real-time traffic, premium data or best-effort data.

Rate limitations are applied at the port and queue levels.

Quality of Service

LA-210 supports Quality of Service (QoS) in DSL egress direction. Classification is according to VLAN priority (802.1p), DSCP (bits 0-5 in IP TOS byte) and port based. Mapping classification results in four transmit priority queues with strict priority, WFQ or both.

Ethernet OAM

LA-210 provides two types of Ethernet OAM:

- End-to-end OAM based on IEEE 802.1ag and ITU T Y.1731 enable Ethernet service providers to monitor their services proactively, measure end-to-end performance and guarantee that the customers receive the contracted SLA. Fault monitoring and performance measurement include Frame Delay, Frame Delay Variation, Frame Loss and Availability
- Single segment (link) OAM according to IEEE 802.3ah fault indication, including remote loopback.

For additional information on OAM, refer to *Appendix C*.

Fault Propagation

When the network to user fault propagation feature is enabled, LAN ports 1, 2 and 3 are deactivated when the PCS uplink becomes unavailable. They will become active again once the PCS port is resynchronized.

Management

The unit can be managed using different ports and applications:

- Remote inband management via the network ports using Telnet, ConfiguRAD or RADview, RAD's SNMP-based management system
- In Bridge mode, Out of band management via one of the user data ports that can be configured as management port
- Local management via an ASCII terminal connected to the RS 232 port.

Management traffic can be separated from user data by creating a dedicated management VLAN.

Up to ten different stations can manage LA-210 monitoring the network status from different locations.

ConfiguRAD

ConfiguRAD is a user-friendly Web-based terminal management system serving for remote device configuration and maintenance. It is embedded into LA-210 and provided at no extra cost. ConfiguRAD can be run from any standard Web browser.

Inband Management

For the inband management, the host of LA-210 can be configured to the tagged or untagged operation: In Flow mode, the SHDSL interface can only be reached via a DSL network and only tagged.

- When the host tagging is enabled, the host packets receive a VLAN tag, creating a dedicated management VLAN.
- When tagging is disabled, no traffic separation is performed and management packets can be forwarded to the user port.

The event log file includes entries at the system and Ethernet levels.

Security

LA-210 ensures client server communication security and correct user authentication using the following protocols:

- RADIUS (client authentication only)
- SSL for Web-based management application
- SSH for Secure Shell communication session
- Management access for Telnet/SSH and Web/SSL can be disabled or restricted to defined managers.
- Automatic logout after 15 minutes of inactivity.

Timing

LA-210 receives the clock signal, derived from the DSL line on a CPE unit.

Statistics

LA-210 provides statistics and counter capabilities in the physical Ethernet and SHDSL level.

1.2 Physical Description

LA-210 is a 1U high standalone device in a plastic enclosure. *Figure* 1-3 illustrates a three-dimensional view of the LA-210 unit. The front and rear panels are shown in *Chapter 3.*

Figure 1-3. LA-210 Front View

The LEDs are located on the front panel. The interfaces and connectors are located on the rear panel. For more information, see *Chapter 2*.

LA-210 is powered by a wide-range AC/DC power supply: 100–240 VAC, 48/60 VDC nominal.

1.3 Functional Description

This section describes the major functional features of LA-210.

Interfaces

This section provides an overview over interfaces available on LA-210.

Ethernet Interface

The Ethernet physical interface is 10/100BaseT. The interface supports autonegotiation.

WAN Interface

The SHDSL interface supports ITU-T G.991.2 and ETSI 101524 standards for SHDSL.

Control Interface

The control port connects directly to an ASCII terminal for locally managing the unit.

Ethernet Access (Bridge Mode)

LA-210 has a multi-port bridging capability handling up to six bridge ports. The Bridge supports two modes of operation:

- VLAN-aware
- VLAN-unaware.

The mechanism of each mode can be described as five different processes:

- Ingress: Checks each frame entering the bridge to decide if and how this frame should be passed on to the forwarding process
- Learning: Learns new MAC table entries (MAC only or MAC VID pairs)
- Aging: Checks the forwarding MAC table periodically
- Forwarding: Decides to which bridge port/ports to forward the frame
- Transmission (VLAN-aware mode only): Selects the format of the transmitted frame at the output port: with VLAN ID (tagged) or without VLAN ID (untagged).

Bridge features and these five processes are described below for each mode.

VLAN-Aware Mode

This mode enables the creation of sub-groups of bridge ports within the bridge. Each sub-group is defined per VLAN and is associated with a unique VLAN ID (VID). Frames containing a VID can be forwarded only between bridge ports that

are members of this specific VLAN, enabling a total separation between different VLAN users within the same bridge.

Bridge Features

- Full VLAN-Aware bridge in accordance with 802.1Q
- Learning and forwarding according to MAC address and VID
- Learning of up to 1,024 MAC table entries (MAC + VID pairs)
- Configuration of the aging time
- MAC table viewing (learned MACs).

Ingress Process

The ingress process is composed of three steps:

- **Frame Admission:** Two modes of operation (configured per bridge):
  - Admit All Frames: All frames arriving from the port are admitted and proceed to the ingress filtering process. PVID is assigned to untagged or priority only tagged frames.
  - Admit Only VLAN Tagged Frames: Only VLAN tagged frames are admitted and allowed to proceed to the ingress filtering process. Untagged or priority-only tagged frames are discarded.
- **Ingress Filtering:** Works in one of the following modes (configured per bridge port):
  - Enable – Performs ingress filtering according to VIDs. Only frames that share a VID assigned to this bridge port are admitted
  - Disable – All frames are forwarded.

    Only admitted frames that pass filtering are submitted to learning and forwarding processes.
- **PVID Assignment:** Is per bridge port configuration:

  In VLAN-Aware mode, each received frame entering the bridge is associated with a single VID. In case the received frame does not contain a VLAN ID (untagged or priority only tagged frames), a specific PVID is assigned to these frames before they pass to the forwarding process.

  Accordingly, the untagged/priority tagged frames that have passed the admission/ingress filtering, are tagged with PVID and proceed to the forwarding process. Tagged frames will be double tagged with the PVID only if Tag Stacking is enabled.

  For untagged frames that were tagged during this process to VID=PVID, the priority tag is assigned at the VLAN priority field, according to the default priority configuration.

  Table 1-2 summarizes the behavior of the ingress process:

Table 1-2. Ingress Process

Frame Admission Mode	Ingress Filtering Mode	Bridge Behavior
Admit all frames	Enable	VLAN tagged frames with a VID (or PVID for untagged/priority tagged frames) that do not include the bridge port in their VLAN member set, are dropped.
	Disable	All frames pass.
Admit VLAN tagged frames	Enable	VLAN tagged frames with a VID that do not include the bridge port in their member set are dropped. Untagged/priority-only tagged frames are dropped.
	Disable	All VLAN tagged frames pass. Untagged/priority-only tagged frames are dropped.

Frames that pass this stage are submitted to the forwarding and learning processes.

Learning Process

The learning process observes the source MAC address (SA) and the VID of the received frame, and updates the forwarding database with the MAC VID pair and with the bridge port that the frame was received from. The Forwarding Data Base (FDB) is also referred to as a MAC table.

Entries in the MAC table can be dynamic (inserted by the learning process) or static (inserted by configuration). A dynamic entry has an aging time associated with it.

The LA-210 VLAN-aware bridge is an Independent VLAN Learning (IVL) bridge.

The learning process inserts a new dynamic entry into the MAC table. This entry consists of a MAC-VID pair and bridge port.

- If the MAC-VID pair already exists for the same port, the aging time is updated
- If the MAC-VID pair already exists but for a different bridge port (dynamic entry), the new entry overrides the existing one
- If the MAC-VID pair already exists for a different bridge port (static entry), the static entry prevails.

Aging Process

The aging process checks the forwarding MAC table periodically. Each dynamic entry-aging period that has exceeded the configured aging time limit is deleted. The aging period represents the time passed since the last frame for this entry entered the bridge. The periodic check of the MAC table (aging time intervals) results in the actual aging time that can reach up to twice the value that was configured by the user.

Forwarding Process

The forwarding process is performed based on the frame destination MAC VID pair. The frame is forwarded to the bridge port that was specified in the MAC table for this MAC VID pair entry.

Untagged frames are forwarded according to the PVID that was attached to that frame during the ingress process.

Frames are forwarded, dropped, or flooded according to the following guidelines:

- Forwarded: If the bridge port of the pair entry (DA, VID) in the MAC table is both an active bridge port and a member of the VLAN, the frame is forwarded to that bridge port only.
- Dropped:
  - If the bridge port for the pair entry (DA, VID) in the MAC table is the port on which the frame was received, the frame is dropped.
  - If there are no active ports associated with the frame's VID, or if the VID is not defined at all, the frame is dropped.
- Flooded:
  - If the pair (DA, VID) is not learned and does not exist in the MAC table, the frame is transmitted to all bridge ports that are associated with the frame's VLAN ID.
  - Multicasts and broadcasts are flooded only through the bridge ports whose VLAN ID is identical to the frame's VLAN ID.

Transmission Process

After the forwarding process identifies the destination bridge port/ports to which the frames must be transmitted, the frames are transmitted in the appropriate format.

The frame format can be configured for each VLAN and port:

- VLAN-tagged: In this mode:
  - VLAN-tagged frames are transmitted unchanged.
  - Untagged frames are transmitted tagged with priority according to the default priority of the ingress bridge port, and VID=PVID of the port from which they entered.
  - Priority-tagged frames are transmitted tagged with original priority and VID = PVID.
- Untagged: In this mode, all frames are transmitted as untagged.

VLAN-Unaware Mode

In this mode the bridge forwarding ignores the VLAN ID of VLAN-tagged frames.

Each Ethernet packet received from each bridge port is forwarded according to its destination MAC address.

Bridge Features

Bridge features include:

- Learning and forwarding according to MAC address only
- Learning of up to 2048 MAC addresses
- Configuration of the aging time
- VLAN tagged frames transparency (forwarding according to MAC only)
- MAC table viewing (learned MACs).

Ingress Process

All frames are accepted in this mode: untagged, priority-tagged, or VLAN tagged.

Learning and forwarding is based on the MAC addresses, with no regard to the VLAN. This mode is also known as transparent mode.

Learning Process

The learning process observes the source MAC address (SA) of the received frame and updates the forwarding database (FDB) with the MAC address and the bridge port that the frame was received from. (FDB is also referred to as MAC table).

The learning process inserts a new entry into the MAC table. This entry consists of the MAC and bridge port.

- If the MAC already exists for the same bridge port, the aging time will be updated.
- If the MAC already exists, but for a different bridge port, (dynamic entry) the new entry will override the existing one.

Aging Process

The aging process checks the forwarding MAC table periodically. Each dynamic entry aging time period that has exceeded the configured Aging Time Limit is deleted. The aging time period is the period of time since the last frame for this entry entered the bridge. The periodic check of the MAC table (aging time intervals), results in an actual aging time that can reach up to twice the value that was configured by the user.

Forwarding Process

The forwarding process is performed based on the frame MAC Destination Address (MDA). The frame is forwarded to the bridge/port specified in the MAC table for this MAC.

Frames are forwarded, dropped, or flooded at this stage:

- Forwarded: A frame will be forwarded according to its DA, to the bridge port where its DA was learned.
- Dropped: If the port for that DA entry in the MAC table is the port on which the frame was received, the frame will be dropped.
- Flooded:
  - If there is no information regarding the DA in the MAC table, the frame is flooded to all ports
  - Frames with multicast or broadcast addresses are flooded to all ports.

Transmission Process

In this bridge mode (VLAN-Unaware), the frames are transmitted unchanged, that is no tags are added or removed.

VLAN Stacking

VLAN Stacking mode for a bridge port refers to the addition of a tag to an incoming frame either at ingress or egress (regardless of whether it already has an existing VLAN tag), and removal of a tag at ingress or egress when the frame leaves from this port.

This setting is independent of the bridge activity.

VLAN Stripping

VLAN Stripping mode for a bridge port refers to the removal of a tag at ingress or egress when the frame leaves from this port.

This setting is independent of the bridge activity.

Ethernet Access (Flow Mode)

Figure 1-4 illustrates the traffic handling process. *Table 1-3* provides an overview of the traffic handling stages.

Each flow can either have a single service assigned to it or up to 8 services which are differentiated by the SP-VLAN P-bits (flow.CoS).

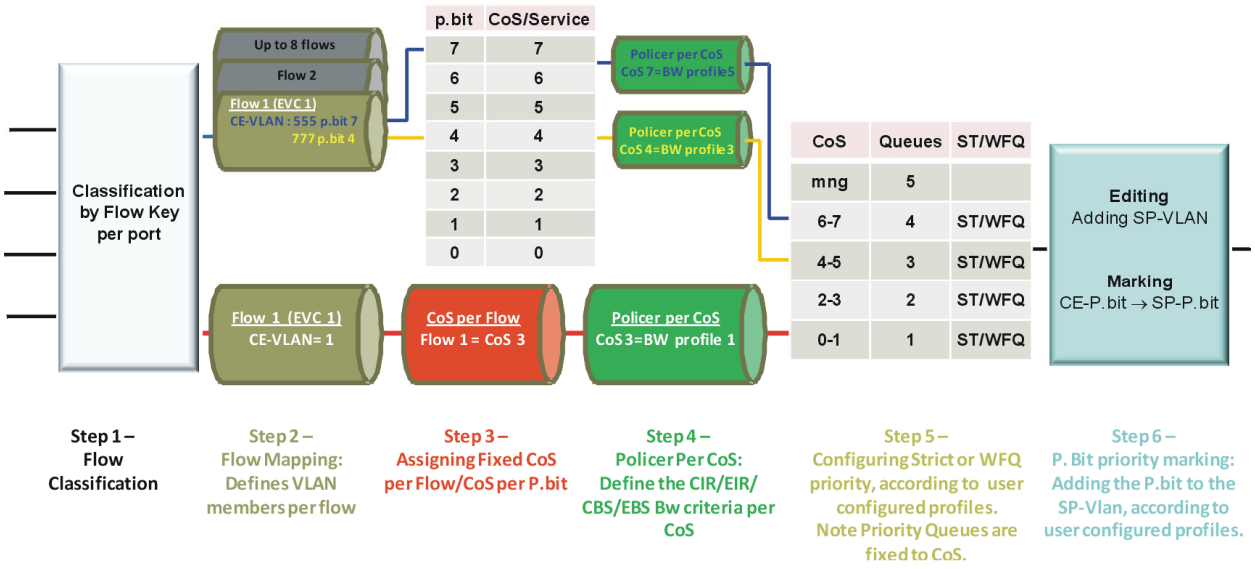

Classification by Flow Key per port
Up to 8 flows
Flow 2
Flow 1 (EVC 1)
CE-VLAN : 555 p.bit 7
777 p.bit 4
p.bit
CoS/Service
7 7
6 6
5 5
4 4
3 3
2 2
1 1
0 0
Policer per CoS
CoS 7=BW profile5
Policer per CoS
CoS 4=BW profile3
CoS
Queues
ST/WFQ
mng 5
6-7 4 ST/WFQ
4-5 3 ST/WFQ
2-3 2 ST/WFQ
0-1 1 ST/WFQ
Editing
Adding SP-VLAN
Marking
CE-P.bit → SP-P.bit
Flow 1 (EVC 1)
CE-VLAN= 1
CoS per Flow
Flow 1 = CoS 3
Policer per CoS
CoS 3=BW profile 1
Step 1 – Flow Classification
Step 2 – Flow Mapping: Defines VLAN members per flow
Step 3 – Assigning Fixed CoS per Flow/CoS per P.bit
Step 4 – Policer Per CoS: Define the CIR/EIR/ CBS/EBS Bw criteria per CoS
Step 5 – Configuring Strict or WFQ priority, according to user configured profiles. Note Priority Queues are fixed to CoS.
Step 6 – P. Bit priority marking: Adding the P.bit to the SP-Vlan, according to user configured profiles.

Figure 1-4. Traffic Handling Diagram

Table 1-3. Traffic Handling Stages

Processing Stage	Description
Classification by Flow Key per Port	Classifying traffic such as email traffic, content streaming, large document transmission etc.
Policer per Flow	Policing the entire traffic within the flow.
CoS/Services	Dividing the services using a 3-bit field, specifying a priority value between 0 (signifying best-effort) and 7 (signifying priority real-time data).
Policer per Service	Policing each Class of Service (CoS).
Queues	'Storing' data that will be transmitted according to the CoS level specified.
Rate Limitation/Shaping	Ensuring that traffic is shaped to the desired rate.
Scheduling	Scheduling and 'regulating' traffic
Editing and Marking	Adding the SP-VLAN, swapping the CE-VLAN or neither, as well as marking the priority on the outer VLAN header.

Quality of Service

LA-210 supports QoS mapping to priority queues (4 PQ, strict priority or WFQ or both, at the network DSL port egress) in the DSL egress direction, according to one of the following:

- VLAN priority (802.1p)
- DSCP (bits 0-5 in IP TOS byte)
- IP Precedence
- Port-based

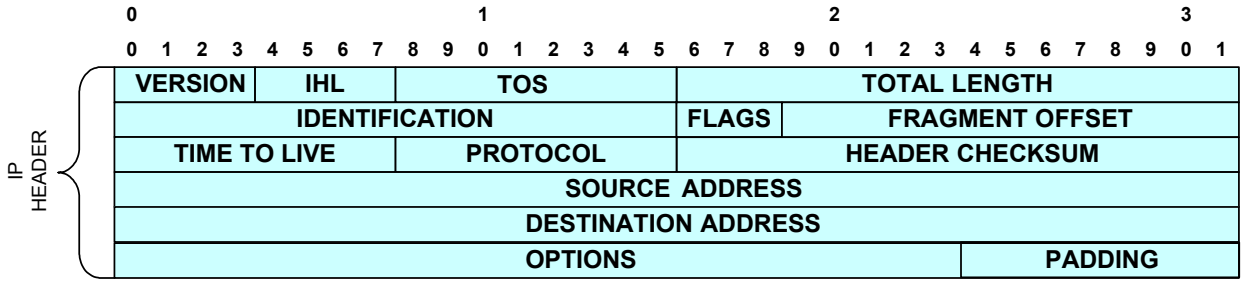


Figure 1-5. IP Header

Bit 0	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
DS5	DS4	DS3	DS2	DS1	DS0	XX	XX

DSCP: six bits (DS5–DS0)

Figure 1-6. ToS Byte DSCP Field

Management

LA-210 performance can be monitored locally from an ASCII terminal, or from a remote site using Telnet or the ConfiguRAD Web-based application. RADview-Lite is also supported.

Inband Management

LA-210 supports inband management via Telnet, SNMP, and Web (ConfiguRAD). Configuration, monitoring, and statistics are available.

Out-of-Band Management

LA-210 enables full configuration and diagnostics via an ASCII terminal. The ASCII terminal is connected to the control port on the rear panel.

For a description of ASCII terminal activation, including general instructions for navigating through the system menus and windows, and modifying data, see *Chapter 3*.

Management Access

The unit's architecture allows access from every bridge port to both the host and remote site devices. In certain configuration modes, a total separation of management traffic from user traffic can be achieved.

VLAN-Based Management Scheme

In this scenario, traffic coming from the remote CPE uses two VLANs: one for user traffic, for which the CPE may use tag stacking, and the other for management traffic. All CPEs connected to the LA-210 share the same management VLAN.

In VLAN-aware mode, LA-210 forwards the management traffic to the management station in the Ethernet network. Because a different VLAN is used, total separation between user traffic and management traffic is maintained.

Statistics

LA-210 provides statistics and counters at the Ethernet and SHDSL levels.

Event Log File

Events are stored and time stamped in an event log file. Up to 1,000 cyclic entries are maintained. The log file is maintained at the Ethernet, SHDSL, and system levels. For more information, see *Chapter 6*.

Diagnostics and Troubleshooting

LA-210 provides several types of diagnostic and troubleshooting procedures:

- Monitoring the system performance
- Displaying status and statistics
- Displaying system messages
- Displaying events/traps

  Traps can be masked per manager IP address, upon user configuration.
- Troubleshooting the device
- Performing connectivity tests
  - Running a ping test
  - Tracing the route

For more information on diagnostics and troubleshooting, see *Chapter 6*.

1.4 Technical Specifications

Line Interface	*Type*	2/4/8-wires unconditioned dedicated line (twisted pair)
	Line Coding	16 or 32 TC-PAM
	Line Rate	192 kbps–5696 Kbps with steps of n × 64 kbps per 2-wires
	*Range** *(26 AWG, noise free)*	• 192 kpbs – 8 km (4.9 miles) • 1536 kpbs – 5.7 km (3.5 miles) • 2048 kpbs – 5.1 km (3.1 miles) • 4096 kpbs – 3.9 km (2.4 miles) • 4608 kpbs – 3.5 km (2.1 miles) • 5696 kpbs – 2.9 km (1.8 miles)
	Impedance	135Ω
	Connector	One RJ-45 per 2 or 4 wires, two RJ-45s for 8 wires RJ-45: Pair 1/3: pins 4, 5, Pair 2/4: pins 3, 6
	Standard	ITU-T G.991.2, ETSI TS 101524
	Protection	ITU-T K.21
Internal Bridge	*Ports*	Fast Ethernet (up to 4)
	LAN Table	Up to 1,024 MAC addresses (static)
	Operation Mode	VLAN-aware, VLAN-unaware
	Filtering and forwarding	Transparent or filter
Control Port	*Interface*	V.24/RS-232
	Type	DCE
	Format	7 or 8 bits; odd, even or no parity
	Baud Rate	9.6, 19.2, 115.2 kbps
	Connector	9-pin, D-type female
Monitoring	*Statistics*	System and physical layer alarms ETH and SHDSL frame counters

		Ethernet physical layer statistics and frame counters
Ethernet Ports	*Interface*	10/100BaseT
	Connectors	1 or 4 RJ-45
Timing		Receive, derived from the SHDSL received signal (CPE unit)
Diagnostics	*Tests*	Ping, trace route
Indicators (Front Panel)	*PWR (green)*	On: LA-210 is powered on Off: LA-210 is off
	TST (yellow)	On: Active test Off: No test
	SHDSL SYNC (green/red)	Blinking (green/red): At least one line is synchronized and at least one line is in process. On (orange): At least one line is synchronized and all others remain unsynchronized and are not in process. On (green): All lines are synchronized Blinking (red): No line is synchronized and at least one line is in process. On (red): No line is synchronized.
	ALM (red)	On: A new alarm is detected in the alarm buffer Off: No alarm currently detected
Indicators (Rear Panel)	***Ethernet Ports***	
	LINK/ACT (green/yellow)	On (green): Ethernet link is up Off: Ethernet link is down Blinking (yellow): Data is being transferred
Power Source	*AC/DC Voltage*	Wide-range: 100–240 VAC, 50/60 Hz or 48/60 VDC nominal (40–72 VDC)
	Estimated Power Consumption (4-Port Unit)	2-wires: 5.9W 4-wires: 6.5W 8-wires: 7W

Physical	*Plastic Enclosure*	
	Height	43.7 mm (1.7 in)
	Width	217 mm (8.5 in)
	Depth	170 mm (6.7 in)
	Weight	0.5 kg (1.1 lb)
Environment	*Temperature*	0° to 50°C (32° to 122°F)
	Humidity	Up to 90%, non-condensing

Chapter 2

Installation and Setup

LA-210 is delivered completely assembled, and is factory set for basic operation. It is designed for installation as a desktop unit or for mounting in a 19-inch rack. For rack installation instructions, refer to the *Rack Mounting Kit for 19-inch Racks* guide that comes with the RM kit.

After installing the unit, use an ASCII terminal connected to the CONTROL port to perform any configuration necessary. The configuration procedures are described in *Chapter 3* and *Chapter 4*.

If problems are encountered, refer to *Chapter 6*.

Warning

No internal settings, adjustment, maintenance and repairs should be performed by either the operator or the user. Such activities must be performed only by skilled personnel who are aware of the hazards involved.

Always observe standard safety precautions during installation, operation, and maintenance of this product.

Note

Before installing the product, review Handling Energized Products at the beginning of the manual.

2.1 Site Requirements and Prerequisites

AC-powered LA-210 units should be installed within 1.5m (5 feet) of an easily accessible grounded AC outlet capable of furnishing the required supply voltage, in the range of 100 to 240 VAC, 50 or 60 Hz.

DC-powered LA-210 units require a -48 VDC power source, which must be adequately isolated from the main supply.

Allow at least 90 cm (36 in) of frontal clearance for operator access. For continuous product operation allow at least 10 cm of frontal clearance and at least 15 cm at rear of the unit, for cable connections and ventilation. For proper ventilation, keep at least 2.5 cm clearance from the sides and top of the product.

The ambient operating temperature of is 0º–50ºC (32º–122ºF), at a relative humidity of up to 90%, non-condensing.

2.2 Package Contents

The package contains the following items:

- One LA-210 unit
- AC power cord or DC adaptor connector
- RM-33-2 rack mount kit for the units in plastic enclosure (if ordered)

2.3 Required Equipment

Hand Tools and Kits

LA-210 needs no special tools for installation. You need a screwdriver to mount the unit in a 19-inch rack.

Power Cable

LA-210 comes equipped with an appropriate (country or region dependent) power cord to be connected from the power socket on the rear panel to the mains.

Cable and Connectors

Refer to the following table to determine what cables and connectors are required for installation. For all connector pinouts, refer to *Appendix A*.

Table 2-1. Required Connection Media

Interface	Cable/Connector
Control port	Straight RS-232/V.24 cable with DB-9 female connector for ASCII terminal
Fast Ethernet interface	RJ-45, 8-pin connection media
SHDSL Interface	RJ-45, 8-pin connection media

2.4 Mounting the Unit

LA-210 is designed for installation as a desktop unit. It can also be mounted in a 19" rack.

- For rack mounting instructions, refer to the RM-33-2 (plastic enclosure) or RM-35 (metal enclosure) installation kit manual.
- LA-210 can be attached to a wall using holes already drilled into the bottom of the enclosure. A drilling template for wall attachments is included at the end of this manual.
- If LA-210 is to be used as a desktop unit, place and secure the unit on a stable, non-movable surface.

Refer to the clearance and temperature requirements in *Site Requirements and Prerequisites*.

2.5 Connecting to SHDSL Equipment

LA-210 can be connected to SHDSL equipment via the single or dual RJ-45 connector, designated SHDSL. Refer to *Appendix A* for the connector pinout.

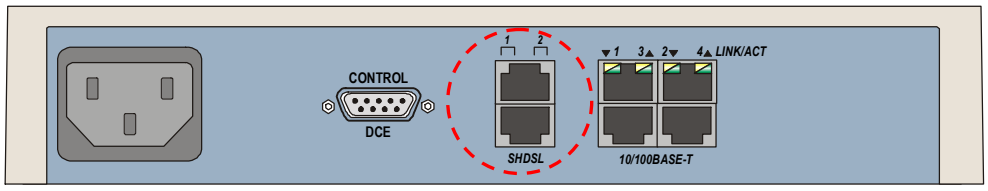


Figure 2-1. Dual SHDSL Connector

➤ **To connect to the SHDSL equipment:**

- Connect LA-210 to the SHDSL equipment using standard straight UTP cables terminated with RJ-45 connectors.

2.6 Connecting to the Ethernet Equipment

LA-210 can be connected to the Ethernet user equipment via one or four 8-pin RJ-45 electrical ports designated ETH. Refer to *Appendix A* for the Ethernet connector pinout.

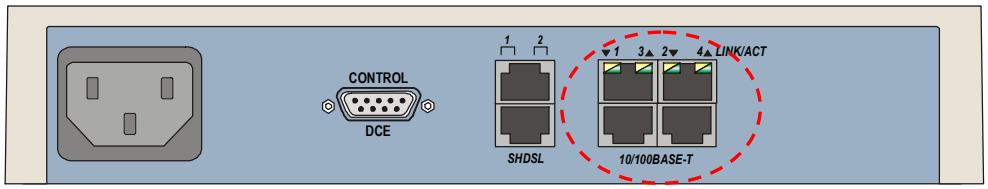


Figure 2-2. 10/100BaseT Connectors

➤ **To connect to the user Ethernet equipment:**

- Connect LA-210 to the user Ethernet equipment using standard straight UTP cables terminated with RJ-45 connectors.

2.7 Connecting to the ASCII Terminal

LA-210 can be connected to an ASCII terminal via a 9-pin D-type female connector designated CONTROL. Refer to *Appendix A* for the connector pinout.

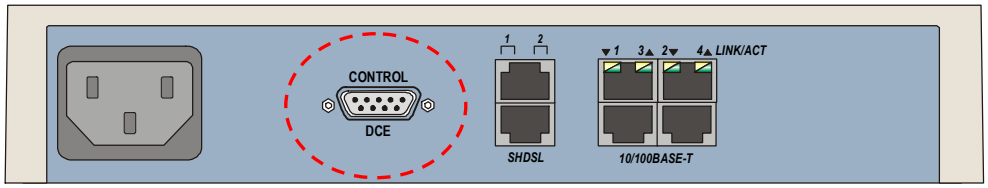


Figure 2-3. CONTROL Connector

➤ **To connect to an ASCII terminal:**

1. Connect the male 9-pin D-type connector of CBL-DB9F-DB9M-STR straight cable available from RAD to the CONTROL connector.
2. Connect the other connector of the CBL-DB9F-DB9M-STR cable to an ASCII terminal.

Caution Terminal cables must have a frame ground connection. Use ungrounded cables when connecting a supervisory terminal to a DC-powered unit with floating ground. Using improper terminal cable may result in damage to the supervisory terminal port.

Note *LA-210 units may be equipped with additional connectors that will be supported by future software versions.*

2.8 Connecting to Power

LA-210 is equipped with a dual input AC/DC power supply. AC or DC power is supplied to LA-210 via a standard 3-prong power input connector on the rear panel.

Warning

Before connecting or disconnecting any communication cable, the unit must be grounded by connecting its power cord to a power outlet with a ground terminal, and by connecting the ground terminal on the panel (if provided) to protective ground.

Any interruption of the protective (grounding) conductor (inside or outside the instrument) or disconnecting the protective ground terminal may render this unit dangerous. Intentional interruption is prohibited.

Connecting AC Power

AC power should be supplied through the 1.5m (5 ft) standard power cable terminated by a standard 3-prong plug. The cable is provided with the unit.

➤ **To connect AC power:**

1. Connect the power cable to the power connector on the LA-210 rear panel.
2. Connect the power cable to the mains outlet.

   The unit turns on.

Connecting DC Power

DC power is supplied to LA-210 via a compatible AC/DC plug for attaching DC power supply lines.

➤ **To connect DC power:**

- Refer to the DC power supply connection supplement for instructions how to wire the DC cables.

Chapter 3

Operation

This chapter provides the following information for LA-210:

- Explains power-on and power-off procedures
- Provides a detailed description of the controls and indicators and their functions
- Provides instructions for using a terminal connected to LA-210's control port
- Describes how to navigate menus
- Describes the configuration alternatives.

For additional information on parameters displayed in the menus, refer to *Chapter 4*.

Before attempting to operate LA-210, make sure to properly complete the installation procedures provided in *Chapter 2* .

3.1 Turning On the Unit

➤ **To turn on the unit:**

- Connect the power cord to the mains.

  The PWR indicator lights up and remains lit as long as LA-210 receives power.

Once installed, LA-210 does not require the operator's attention, with the exception of occasional monitoring the front panel indicators. Intervention is only required when the unit must be configured to its operational requirements, or when it is being tested.

3.2 Indicators

The LED indicators are located on the front panel as illustrated in *Figure 3-1*. *Table 3-1* lists the functions of the LA-210 LEDs.

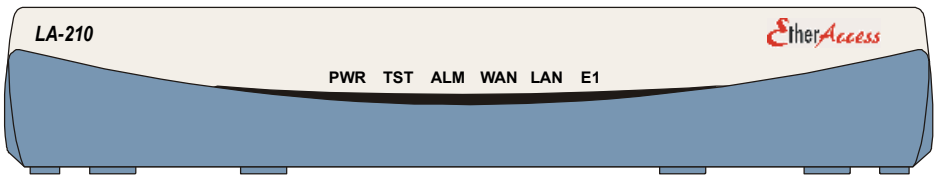


Figure 3-1. LA-210 Front Panel (Plastic Enclosure)

Table 3-1. LA-210 LEDs

Name	Function
PWR (green)	On: LA-210 is on Off: LA-210 is off
TST (red)	On: A test is active Off: A test is inactive
ALM (red)	On: A new alarm is detected in the alarm buffer Off: No alarm currently detected
WAN (SHDSL SYNC 1, 2, 3, 4 - green/yellow)	On (green): At least one SHDSL line is synchronized and ready to transmit data. Flashing (green): No SHDSL line is synchronized. At least one SHDSL line is being initialized. Flashing (yellow): No SHDSL line synchronized or being initialized. At least one SHDSL line is in PAF establishment stage. On (yellow): No SHDSL line synchronized and no SHDSL being initialized or in PAF establishment stage.
LAN (LINK/ACT – green/yellow)	On (green): Ethernet link is up Off: Ethernet link is down Blinking (yellow): Data is being transferred
E1	Off: Not used

3.3 Default Settings

Table 3-2 lists the default settings of the LA-210 configuration parameters.

Table 3-2. Default System Settings

Menu	Parameter	Default Value
System	Applixation Mode	Bridge Mode
Management		
Device Information	Description	LA-210, HW Version 0.00, SW Version 1.50D9
	Name	LA-210
	Location	Location of the device
	Contact	Name of the contact person
Host	IP Address	0.0.0.0
	Mask	255.255.255.0
	Default Gateway	0.0.0.0

Menu	Parameter	Default Value
	Read Community	Public
	Write Community	Private
	Trap Community	Public
Encapsulation	Host Tagging	Untagged
	Host VLAN ID	-
	Host Priority Tag	0
Management Access		
User Access	Old User Name	USER ; SU
	New User Name	Empty string
	Old Password	1234
	New Password	Empty string
	Confirm New Password	Empty string
	Telnet Access/SSH Access	Enable
	SNMP Access	Enable
	Web Access	Enable
Radius Parameters	Server Status	Not Connected
	Server Access	Disable
	Server IP Address	0.0.0.0
	Key String	Empty string
	Number of Retries	2
	Timeout	2 sec
	Authentication Port	1812
Terminal	Baud Rate	9600 bps
Fault Propagation	Network → User	Disable
	User → Network	Disable
Date and Time	Date	0000-00-00
	Time	0:00:00
	NTP Mode	Disable
	GMT	0
	NTP Server IP Address	0.0.0.0
	NTP Update Interval	0
Physical Layer		
Ethernet	Port	1

Menu	Parameter	Default Value
	Administrative Status	Up
	Auto Negotiation	Enable
	Flow Control	Disable
	Max Capability Advertised	100BaseTX full-duplex
	Speed & Duplex	100BaseTX full-duplex
	MDIX Cross Over	Enable
	OAM (EFM)	Disable
	Ingress Rate Limit	100000 kbps
	VLAN Tag Ether Type	8100
SHDSL		
Line	Line	1
	Administrative Status	Up
	Wire Mode	2-Wire
	Line Ptobe	Enable
	TC Layer	64-65 Octet
	Power Backoff	0 (Off)
	Current Marging	0 (Disable)
	Worst Margin	0 db
	Loop Attenuation Threshold	0 db
	SNR Marging Threshold	0 db
PCS	PCS	1
	Administrative Staus	Up
	OAM (EFM)	Disable
	Egress Rate Limit	100000
	VLAN Tag Ether Type	8100
Applications (Bridge Mode)		
Bridge	VLAN Mode	Unaware
	Forwarding Mode	Filter
	Aging Time	300 sec.
Bridge Port	Bridge Port	2

Menu	Parameter	Default Value
	Activation	Enable
	Port VID/Stacking VID	2
	Copy Original Priority	Disable
	Default Priority tag	0
	Egress Tag Handling	None
	Ingress Filtering	None
VLAN Membership	VLAN ID	Empty string
	Egress Tagged Ports	Empty string
	Egress Untagged Ports	Empty string
Bind	Ethernet Port [#] / PCS [#]	1
QoS	Priority Classification	802.1p
Priority Mapping	User Priority 0	Traffic Class 0
	User Priority 1	Traffic Class 0
	User Priority 2	Traffic Class 0
	User Priority 3	Traffic Class 0
	User Priority 4	Traffic Class 0
	User Priority 5	Traffic Class 0
	User Priority 6	Traffic Class 0
	User Priority 7	Traffic Class 0
Queue Profiles	ID	1
	Name	QdefaultProfile1
Internal Queues	Internal Queue	1
	Scheduling	Strict
	Egress Rate Limit	100000 kbps
OAM		
End-To-End	Standard OAM MAC Address	0180C2000030
	Standard OAM EtherType	8902
	Flows	0
MD Names	MD ID	1
	MD Format	None
Flows	Flow	0
	Flow Name	Empty string
	SP VLAN	1
	Protocol Type	Standard

Menu	Parameter	Default Value
MAID	Flow ID	Empty string
	MD ID	1
	MD Format	None
	MD Name	None
	MA Format	String
	MA Name	Default
MEP	Flow ID	Empty string
	Local ID	0
	OAM Destination Address Type	Multicast
	Remote ID	Empty string
	MD Level	3
	OAM Mode	Disable
	CC Interval	1 second
Applications (Flow Mode)		
QoS		
CoS Profiles	ID	1
	Name	CoSDefaultProfile1
	Ingress Priority Method	IEEE 802.p
	Mapping	Tag 0 [0 – 7] Tag 1 [0 – 7] Tag 2 [0 – 7] Tag 3 [0 – 7] Tag 4 [0 – 7] Tag 5 [0 – 7] Tag 6 [0 – 7] Tag 7 [0 – 7]
Marking Profiles	ID	1
	Name	MarkingDefaultProfile1
	Method	IEEE 802.p

Menu	Parameter	Default Value
	Marking	Tag 0 [0 – 7] Tag 1 [0 – 7] Tag 2 [0 – 7] Tag 3 [0 – 7] Tag 4 [0 – 7] Tag 5 [0 – 7] Tag 6 [0 – 7] Tag 7 [0 – 7]
Bandwidth Profiles	ID	1
	Name	DefaultIngressBW1
	CIR	99968 kbps
	CBS	12176 bytes
	EIR	0
	EBS	12176 bytes
Queue Profiles	ID	1
	Name	QdefaultProfile1
Internal Queues	Internal Queue	1
	Scheduling	Strict
	Weight	50
	Egress Rate Limit	100000 kbps
Flows		
Flow Interfaces	Interface ID	1
	Port	ETH-1
	Flow Key	CE-VLAN ID
Flow Definition	ID	1
	Name	Empty string
	Interface	1
	User Port Mapping Mode	User Mapping
	CoS Method	Profile
	CoS Value	1
	CoS Profile	CoSDefaultProfile1
	Ingress BW Profile	Undefined
Encapsulation	SP-VLAN Action	Stacking
	SP-VLAN	0
	Marking Method	Profile

Menu	Parameter	Default Value
	Marking Profile	MarkingDefaultProfile1
	CE-VLAN Action	Preserve
CoS	ID	0
	Name	Empty string
	Ingress BW Profile	Undefined
OAM		
End-To-End		
	Standard OAM MAC Address	0180C2000030
	Standard OAM Ether Type	8902
MD Names	MD ID	1
	MD Format	None
Flows	Flow	1
	Flow Name	Empty string
	SP VLAN	1
	Protocol Type	Standard
MAID	Flow ID	Empty string
	MD ID	1
	MD Format	None
	MD Name	None
	MA Format	String
	MA Name	Default
MEP	Flow ID	Empty string
	Local ID	0
	OAM Destination Address Type	Multicast
	Remote ID	Empty string
	MD Level	3
	OAM Mode	Disable
	CC interval	1 second
	MA Name	Default

3.4 Configuration and Management Alternatives

After installation, there are no special operating procedures for LA-210. Once it is powered up, the unit operates automatically. The unit operational status can be monitored constantly.

If required, LA-210 can be reconfigured, using different ports and applications:

- Local out-of-band management via an ASCII terminal connected to the RS-232 port. Usually, preliminary configuration of the system parameters is performed via ASCII terminal. Once the LA-210 host IP parameters are set, it is possible to access it via Telnet, ConfiguRAD or RADview for further configuration.
- Remote inband management via user or the network ports. Remote management is performed using Telnet, or ConfiguRAD (RAD's Web-based management application), or RADview (RAD's SNMP-based management system). Alternatively, LA-210 can be managed via a third-party SNMP-based NMS (refer to *Chapter 6* for a list of traps).

Working with Terminal

LA-210 includes a V.24/RS-232 asynchronous DCE port designated CONTROL, which is terminated in a 9-pin D-type female connector. The control port continuously monitors the incoming data stream and immediately responds to any input string received through this port.

The control port can be configured to communicate at the following rates: 9.6, 19.2, or 115.2 kbps.

➤ To start a terminal control session:

1. Make sure all cables and connectors are properly connected.
2. Connect the unit to a PC equipped with an ASCII terminal emulation application (for example, Windows Hyper Terminal or Procomm).
3. Turn on the control terminal PC and set its default port parameters to 9,600 baud, eight bits/character, one stop bit, and no parity.
4. Set the terminal emulator to ANSI emulation (for optimal view of system menus).
5. Set the terminal emulator to view a 132-character screen width.
6. When the initialization and self-test are over, a menu appears displaying initialization and self-test results.

Logging In

➤ To log in:

1. Enter **su** for user name with read/write permission.
2. Enter **1234** for (default) password.

Note *It is recommended to change default passwords to prevent unauthorized access to the unit.*

Choosing Options

➤ To choose an option:

1. Press the number corresponding to the option, and press <**Enter**>.
2. Press <**S**> to save your changes.

   LA-210 updates its database with a new value or displays a new menu for the selected option.
3. If you press <**ESC**> to exit the menu without saving your changes, the following message appears:

   "Do you want to save changes (Y/N/C)?"

   Press the appropriate letter to save or not save your changes (**Y**es/**N**o/**C**ancel).

Note *When a menu option has only two values, typing the option number and pressing <**Enter**> will toggle between the available values.*

Screen Example

The following figure shows a typical screen with main items displayed.

```
                    Product title line (LA-210)
                           Short message
1. Sub Menu>
2. Sub Menu>
3. Parameter X [Range] …… (value)
4. Parameter Y>            (Select value from the list)
5. Table Z []

prompt>
Main>Configuration>System>

Help line message
Help line of keyboard shortcuts, such as "Esc-prev" for
returning to the previous menu
-----------Division screen line ------------------
Scroll messages
```

Figure 3-2. Sample Screen

Navigating Tables

Some screens, such as the Manager table, consist of tables and are larger than regular menus and may require scrolling to navigate between parameters. These screens are best viewed when your terminal screen is set to 132 character width.

Use the following keys (case-sensitive) for table navigation:

Table 3-3. Table Navigation Keys

Key	Navigation
<Ctrl>+L	Move left
Left Arrow	Move left
<Ctrl>+R	Move right
Right Arrow	Move right
Up Arrow	Move up
Down Arrow	Move down
<Tab>	Select the next changeable cell
G<row number>, <col number>	Go to the specified cell

Note

*You can display these navigation keys by pressing <**?**> from a table.*

The following figure shows a static MAC table in VLAN-aware mode. For VLAN-unaware bridges, the "VLAN ID" column is not displayed. VLAN ID, MAC address, and Receive Bridge port are the columns of the parameters to be defined.

The "A – Add ; R – Remove ; C – Clear" line appears when at least one entry is configured. If the table is empty, only "A - Add" appears.

```
                                LA-210
Main Menu>Configuration>Applications>Bridge>Static MAC table

      VLAN ID       MAC address             Receive Bridge port

  1     1           11-11-11-11-11-11             1
| 2     1           22-22-22-22-22-22             2
v 3     2           33-33-33-33-33-33             3
  4     3           44-44-44-44-44-44             3
  5     4           55-55-55-55-55-55             5

1. MAC address … (11-11-11-11-11-11)

A – Add ; R – Remove ; C – Clear
ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 3-3. Sample Table Screen (Static MAC Table)

Help Screen Example

The following figure shows a typical Help screen, which summarizes the keyboard shortcuts that are available in the functional screen from which the Help screen was invoked.

The Help screen appears upon pressing <**?**> from the relevant functional screen. If a screen is not associated with a help screen, an error is returned.

```
                          Table Hot Keys

'L'  - move left
'd'  - scroll down       'D' - move down
'a'  - add row           't' - remove row
'm'  - represent entry as menu
'c'  - clear table
TAB  - select next changeable cell

S <row number>,<col number> - select cell
```

Figure 3-4. Typical Help Screen

Working with ConfiguRAD

ConfiguRAD is a Web-based remote access terminal management software. It provides a user-friendly interface for configuring, collecting statistics and performing diagnostic tests on the unit.

Web Browser Requirements

The following Web browsers can be used to access the LA-210 ConfiguRAD supervision utility from any location using Internet protocols.

- Internet Explorer version 6.0 and up, running on Windows™ 98, Windows™ 2000, Windows™ XP
- Netscape Communicator version 7.1 and up, running on Windows™ NT or Unix
- Firefox version 1.0.4 and up
- Mozilla version 1.4.3 and up.

Logging In

➤ To log in via Web browser:

1. Connect the Ethernet port to the LAN.
2. Open the Web browser.
3. Disable any pop-up blocking software, such as Google Popup Blocker.
4. Enter the IP address of the LA-210 in the address field of the browser in the following format: **http://'IP address'** (**'IP address'** stands for the actual LA-210 IP address which has to be assigned via an ASCII terminal).
5. Press ‹**Enter**› to command the browser to connect.
6. After the opening window is displayed, click **LOGIN**.
7. In the Password Entry window, enter your user name (read/write user default is **su**) and password (default is **1234**).

   The ConfiguRAD Main menu is displayed.

Note

- *It is recommended to change default passwords to prevent unauthorized access to the unit.*
- *LA-210 allows six management sessions to be active simultaneously: one network session (Telnet, ConfiguRAD, RADview-Lite) and one ASCII terminal session.*
- *If no user input is detected for 5 minutes during a ConfiguRAD session, LA-210 automatically disconnects from the management station.*

Navigating the ConfiguRAD Menus

At the left-hand bottom corner, ConfiguRAD provides auxiliary management tools:

- **Status** – shows the number of users currently managing the unit.
- **Trace** – opens an additional pane for system messages, progress indicators (ping, software and configuration file downloads) and alarms.
- **Refresh All** – refreshes the data currently displayed.

➤ **To choose an option:**

1. Click a link in the ConfiguRAD screen to display the next menu.
2. Once the target screen is displayed, select a value from the drop-down box or enter it in a text box.

Menu Map

Use the menu maps on the following pages as a reference aid when performing configuration and control functions (see *Figure 3-5* - *Figure 3-7*).

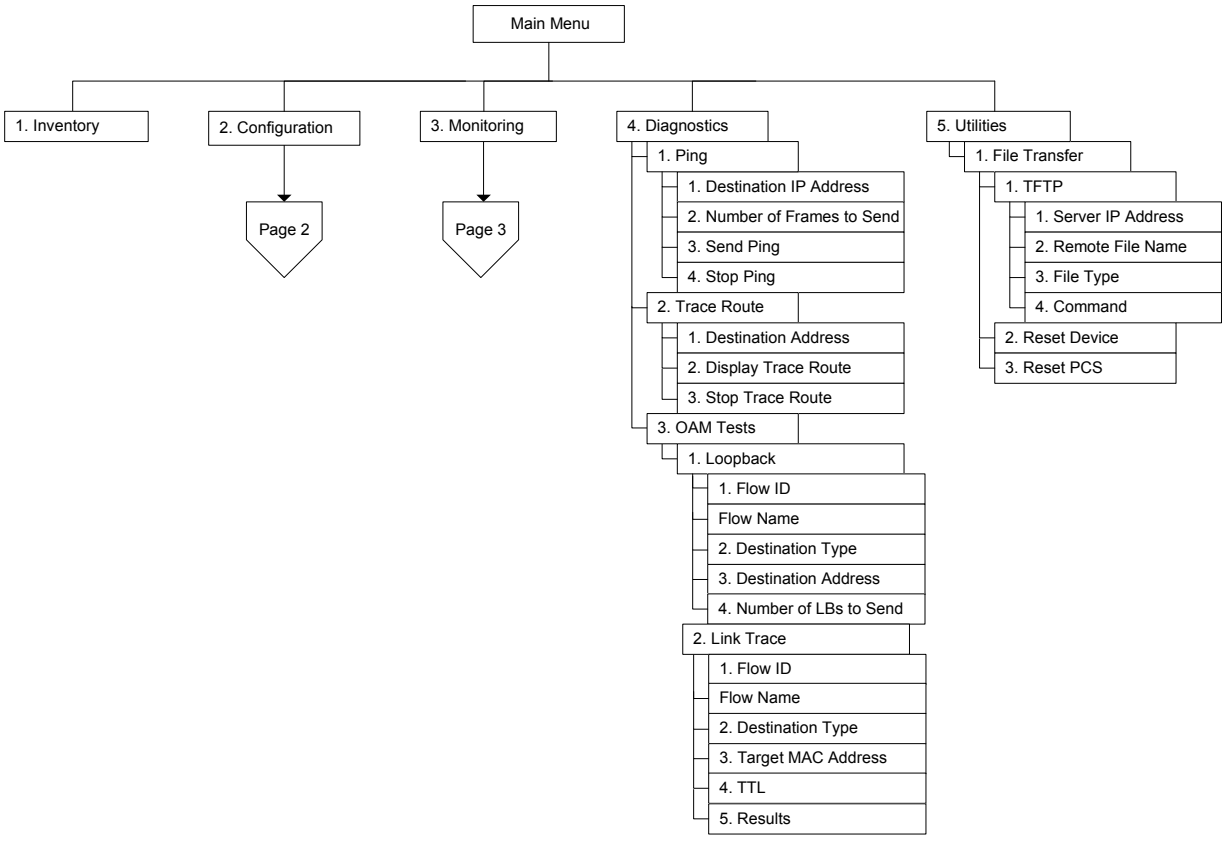


Figure 3-5. Main Menu Map

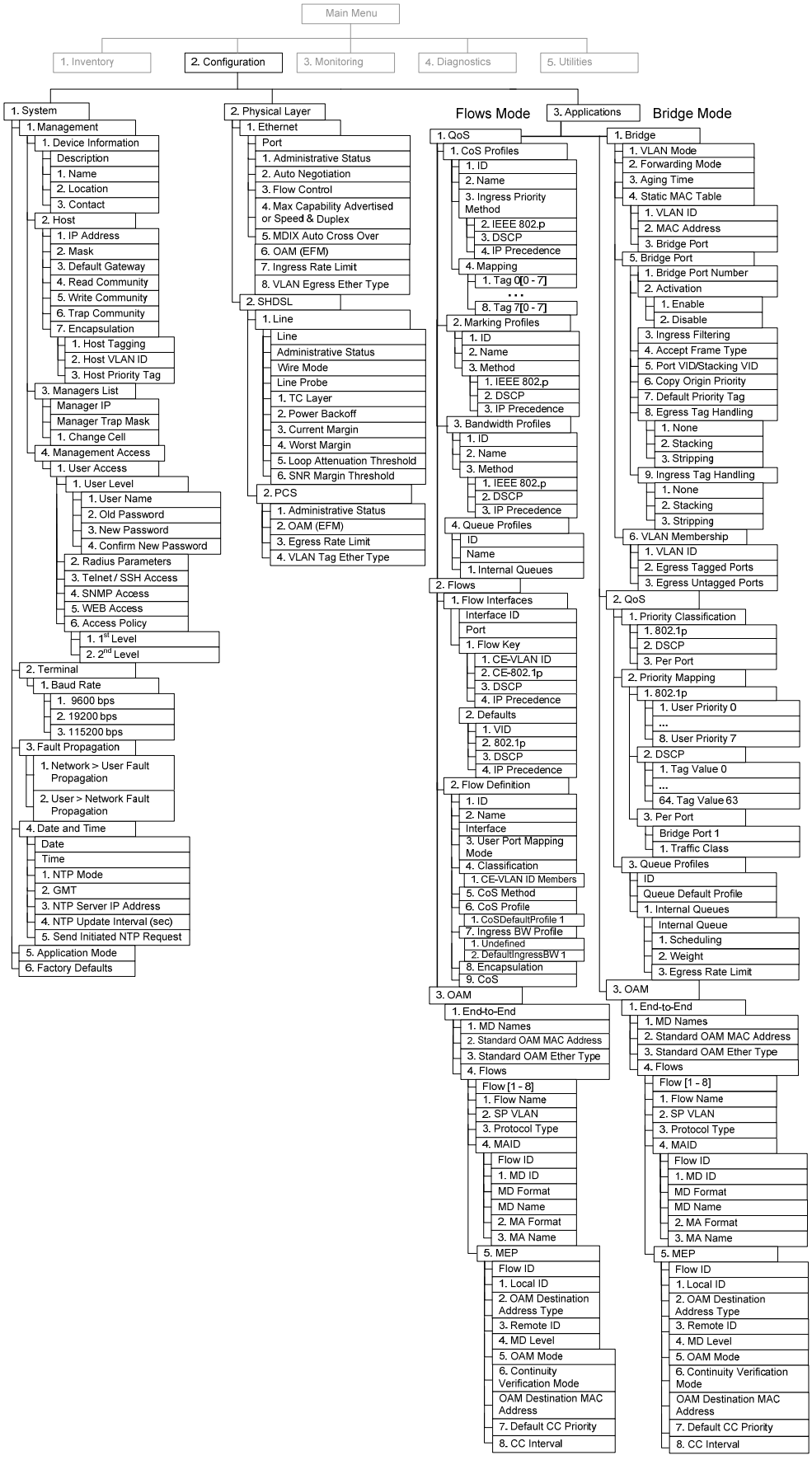


Figure 3-6. Configuration Menu Map – Page 2

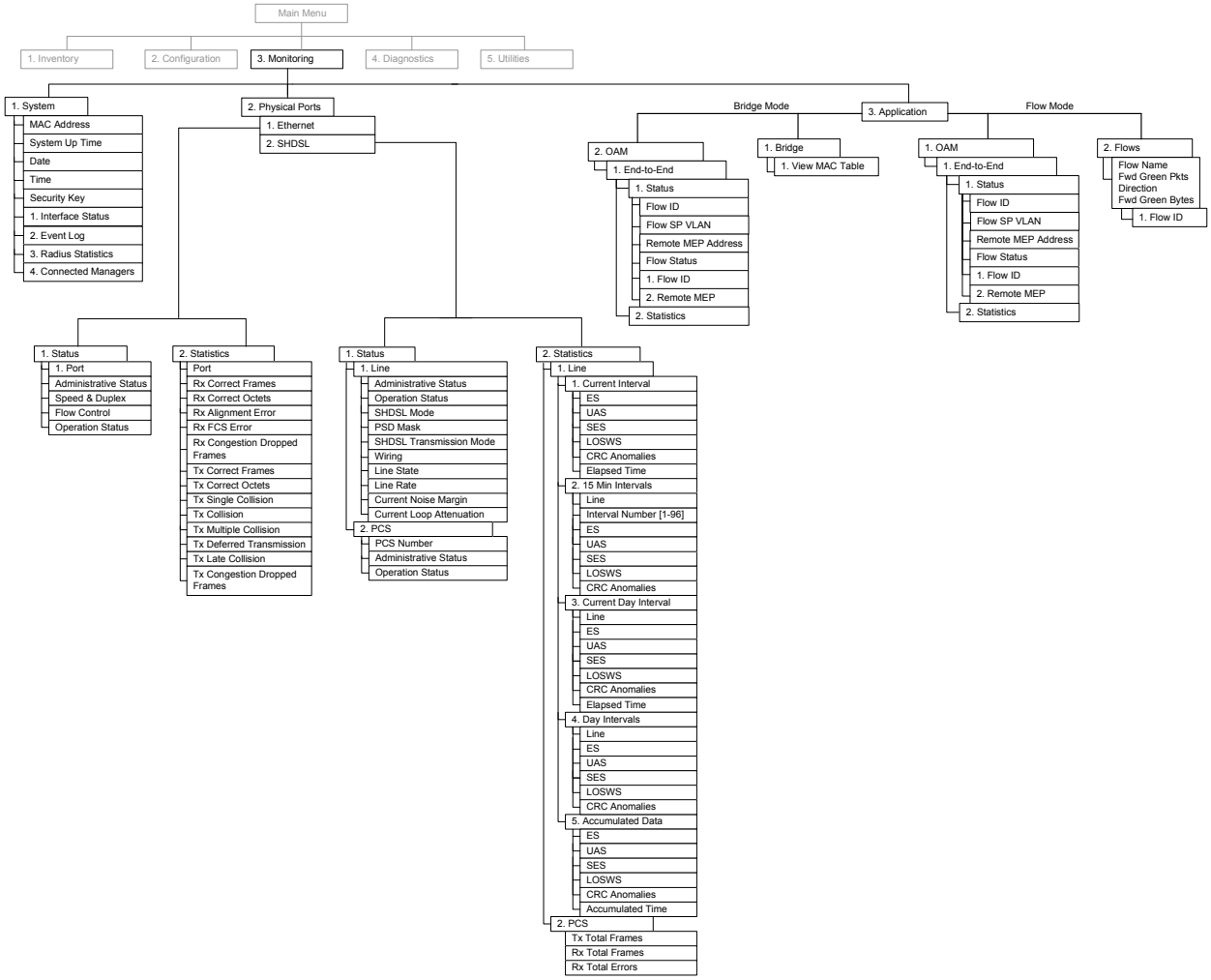


Figure 3-7. Monitoring Menu Map – Page 3

3.5 Turning Off the Unit

➤ To power off the unit:

- Remove the power cord from the power source.

Chapter 4

Configuration

This chapter describes how to configure the LA-210 for management and operational tasks. Configuration screens are shown, and configuration parameters explained.

Note *The configuration screens illustrated in this chapter are taken from a terminal screen, but most of the menus are similar to those viewed in Telnet and ConfiguRAD.*

This chapter includes the following sections:

- Configuring for management (*page 4-1*)
- Configuring for operation (*page 4-10*)
- Additional tasks (*page 4-39*).

For instructions on accessing and navigating the screens, and a complete list of all menu items, refer to *Chapter 3*.

4.1 Configuring for Management

This section describes how to configure the LA-210 for management functions.

Entering Device Information

The LA-210 management software allows you to assign a name for the unit, and specify its location to distinguish it from the other devices installed in your system. A contact person can also be assigned. Each of these fields can hold up to 50 characters.

➤ **To enter device information:**

- From the Device Info menu (Configuration › System › Management › Device Information), perform the following:
  1. Select **Device Name,** and type a name for the unit.
  2. Select **Location**, and type a location name/description.
  3. Select **Contact Person**, and type the name of a contact person for this unit.

```
                                    LA-210
Main Menu > Configuration > System > Management > Device Information

   Description                 … (LA-210, HW Version 0.00, SW Version 1.50D5)

1. Name                        … (LA-210)
2. Location                    … (Location of the device)
3. Contact                     … (Name of the contact person)

S - Save
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-1. Typical Device Information Screen

Configuring IP Host Parameters

You can manage the unit via a network management station connected to one of the unit's ports. To establish a proper connection, it is necessary to configure the Host IP parameters. In addition, by selecting a forwarding mode and VLAN parameters, it is possible to create a separate management VLAN.

➤ To define the Host parameters:

1. From the Host IP menu (Configuration › System › Management › Host), perform the following:
   - Select **IP Address** and enter the IP address of the IP host.
   - Select **IP Mask** and enter the host IP subnet mask.
   - Select **Default Gateway** and enter the default gateway IP address.
   - Select **Read Community** and type the name of a community with read-only authorization.
   - Select **Write Community** and type the name of a community with write authorization.
   - Select **Trap Community** and type the name of a community to which the unit should send traps.
   - Select **Encapsulation** to define VLAN tagging performed by the host.
   - The Encapsulation screen appears (see *Figure 4-3*).
2. From the Encapsulation menu (Configuration › System › Management › Host IP › Encapsulation), perform the following:
   - Select **Host Tagging** and toggle between Untagged and Tagged.
     - **Untagged** – The host sends and receives frames with no VLAN tag to/from the bridge.
     - **Tagged** – The host receives frames only when they are tagged with the host's VLAN ID, and it sends frames to the bridge with this tag.

Note *When Host Tagging is set to **Tagged**, two parameters are added to the menu: **Host VLAN ID** and **VLAN Priority**.*

   - Select **Host VLAN ID** to specify the host VLAN ID (1–4094).

- Select **VLAN Priority** to specify the priority level for the host VLAN (0–7).

```
                              LA-210
Configuration > System > Management > Host

1. IP Address                          … (172.17.143.140)
2. Mask                                … (255.255.255.0)
3. Default Gateway                     … (172.17.143.1)
4. Read Community                      … (public)
5. Write Community                     … ()
6. Trap Community                      … ()
7. Encapsulation                       >

S - Save
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-2. Host IP Screen

```
                              LA-210
Configuration > System > Management > Host > Encapsulation


1. Host Tagging                          > (Tagged)
2. Host VLAN ID [1-4094]                 … (2)
3. Host Priority Tag [0-7]               … (0)

S - Save
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-3. Encapsulation Screen

Selecting the Terminal Baud Rate

The supervisory terminal is connected to LA-210 via the control port. The management software allows you to configure the terminal baud rate.

Note *The Baud Rate parameter is masked during a Telnet session.*

➤ **To select the terminal baud rate:**

- From the **Terminal** menu (Configuration › System › Terminal), select **Baud Rate** and select the desired baud rate of the control port. The following baud rates are available:
  - 9600 bps (default)
  - 19200 bps
  - 115200 bps.

```
                              LA-210
Configuration > System > Terminal

1. Baud rate                    > (9600 bps)

S - Save
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-4. Terminal Screen

Configuring Management Access

You can enable or disable access to the LA-210 management system via an SNMP, Telnet or Web-based application. By disabling SNMP, Telnet or Web, you prevent unauthorized access to the system when security of the LA-210 IP address has been compromised. When SNMP, Telnet and Web access is disabled, LA-210 can be managed via an ASCII terminal only.

➤ To modify Telnet, SNMP, or WEB access permissions for a user:

- From the Management menu (Configuration › System › Management), select Management Access.

  The Management Access menu appears as illustrated in *Figure 4-5*.

```
                              LA-210
Configuration > System > Management > Management Access

1. User Access                          >
2. Radius Parameters                    >
3. Telnet/SSH Access                    (Enable)
4. SNMP Access                          (Enable)
5. WEB Access                           (Enable)
6. Access Policy

ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-5. Management Access

➤ To configure Telnet access:

- Select Telnet and then choose as follows:
  - Enable – All users are enabled.
  - Managers Only – Managers listed in the Managers list are enabled.
  - Secure – Users using an SSH connection are enabled.
  - Managers Only Secure – Managers listed in the Managers list using an SSH connection are enabled.
  - Disable – Telnet access is disabled.

➤ To configure SNMP access:

- Select SNMP and then choose as follows:
  - Enable – All users are enabled.

- **Enable Managers Only** – Managers listed in the Managers list are enabled.
- **Disable** – SNMP access is disabled.

➤ **To configure Web access:**

- Select **WEB** and then choose as follows:
  - **Enable** – All users are enabled.
  - **Enable Managers Only** – Managers listed in the Managers list are enabled.
  - **Secure** – Users using an SSL connection are enabled.
  - **Secure Managers Only** – Managers listed in the Managers list using an SSL connection are enabled.
  - **Disable** – Web access is disabled.

Configuring Radius Server Parameters

LA-210 provides connectivity to up to four Radius authentication servers.

➤ **To configure Radius server parameters:**

1. From the Management menu (Configuration > System > Management), select **Radius Parameters**.

   The Radius Server menu appears as illustrated in *Figure 4-6*.

2. Specify the following parameters according to *Table 4-1*:
   - **Server Access**. Enable or Disable
   - **Server IP Address**. The Radius server's IP address
   - **Key String**. Shared secret
   - **Number of Retries and Timeout**. Access-attempt parameters
   - **Authentication Port**. Port used for authentication.
3. To switch to additional Radius servers, press <**F**> or <**B**> respectively.

```
                              LA-210
Configuration > System > Management > Management Access >
Radius Parameters

   Server Sequence Number                    (1)
   Server Status                        >    (NOT_CONNECTED)
1. Server Access                             (Disable)
2. Server IP Address                    ...  (0.0.0.0)
3. Key String                           ...  ()
4. Number of Retries[0 - 10]            ...  (2)
5. Timeout (in seconds)[1 - 5]          ...  (2)
6. Authentication Port[1 - 65535]       ...  (1812)

Please select item <1 to 6>
F - Forward; B - Backward
ESC-prev.menu; !-main menu; &-exit
```

Figure 4-6. Radius Parameters

Note *The Radius functionality requires LA-210 be connected to a Radius authentication server maintained by a trained technician. This server should be configured in consultation with this technician.*

Table 4-1. Radius Parameters

Parameter	Possible Values	Remarks
Server Sequence Number	1-4 The default is 1	Sequential Radius server number
Server Status	Connected Not connected (default) Disconnecte	Radius server connection status
Server Access	Disable (default) Enable	Enable or disable access to the Radius server
Server IP Address	0.0.0.0 to 255.255.255.255 The default is 0.0.0.0	IP address of the Radius server
Key String	User name (case sensitive)	Shared secret between Radius server and user. It is used for encryption
Number of Retries	1-10 The default is 2	Max. number of access attempts
Timeout	1-5 The default is 2	Number of seconds before access attempt fails
Authentication Port	1-65535 The default is 1812	Authentication protocol port

Defining the Access Policy

Access policy allows configuration of multiple authentication protocols. User authentication is performed in the order the methods are selected. If the first authentication method is not available, the next selected method is used.

➤ **To define the access policy:**

- From the Management Access menu (Configuration › System › Management › Management Access), select **Access Policy**.

  The Access Policy menu appears as illustrated in *Figure 4-7* and *Table 4-2.*

```
                                LA-210
Configuration > System > Management > Management Access >
Access Policy

 1. 1st Level                                  (Local)
 2. 2nd Level                                  (Local)

ESC-prev.menu; !-main menu; &-exit
```

Figure 4-7. Access Policy

Table 4-2. Access Policy

Parameter	Possible Values	Remarks
1st Level	Local Radius	• Local: LA-210 uses the locally stored authentication database • Radius: LA-210 uses the authentication database stored on the Radius server. If you select **Radius**, **2nd Level** becomes available. If the user name is not found in the Radius Server database or the password you enter does not match the user name, the authentication fails. **Default: Local**
2nd Level	None Local	• None: LA-210 is only available via the first level. • Local: LA-210 uses the locally stored authentication database. **Default: Local**

Configuring the Network Managers

The network management stations to which the SNMP agent sends traps can be defined or modified. Up to ten managers can be defined. Entering the IP address and corresponding subnet mask defines each management station. In addition, you can temporarily prevent a manager station from receiving traps by masking the network manager.

➤ To edit the manager list:

1. In the Managers List menu (Configuration › System › Management › Managers List), press ‹A› to add a new network manager,
2. Move the cursor to the **Manager IP** cell you wish to modify by pressing the **Tab** key. The selected cell is highlighted and the value appears in the **Change cell** field.
3. Select **Change Cell**, and press ‹**Enter**› to enter a new IP address for the selected network manager.
4. Move the cursor to the **Trap** field and toggle between **Mask** and **Unmask** to mask or unmask traps for the selected management station.

```
                              LA-210
Configuration > System > Management > Managers List

                    IP address            Trap
  1.                 1.1.1.1              Unmask
| 2.                 2.2.2.2              Unmask
v 3.                 3.3.3.3              Mask
  4.                 4.4.4.4              Unmask
  5.                 5.5.5.5              Unmask

1. Change cell                         … (1.1.1.1)

ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 4-8. Manager List Screen

```
                              LA-210
Configuration > System > Management > Managers List

Manager IP Mask          ... (255.255.255.0)
Manager Trap Mask        ... (Enable)
Save All
 >

ESC-prev menu; !-main menu; &-exit;                        1 user(s)
```

Figure 4-9. Manager List Screen, Add Mode

4.2 Configuring for Operation

This section explains how to configure the unit for operation. This includes the following:

- System level parameters:
  - Fault propagation (*page 4-10*)
  - Date and time, NTP client configuration (*page 4-11*)
  - Application mode, selecting the Bridge or Flows mode (*page 4-11*)
- Physical layer parameters:
  - Fast Ethernet interfaces (*page 4-13*)
  - SHDSL interfaces (*page 4-15*)
- Application layer parameters:
  - Bridge (*page 4-17*)
  - QoS (*page 4-23*)
  - Flows (*page 4-25*)
  - OAM (*page 4-34*).

Setting System Level Parameters

This section includes procedures for setting the configuring fault propagation options.

Configuring Fault Propagation

When the network › user fault propagation is enabled, the LAN ports are deactivated when the PCS uplink becomes inactive. The Ethernet ports are re-activated once the PCS port synchronization is restored.

When the user › network fault propagation is enabled, the PCS uplink is deactivated when the LAN ports become inactive. The PCS uplink is restored once the LAN ports are re-activated.

➤ **To configure the fault propagation:**

- In the Fault Propagation menu (Configuration › System › Fault Propagation), enable or disable the network-to-user or user-to-network fault propagation.

```
                              LA-210
Configuration > System > Fault Propagation

1. Network - >  User Fault Propagation   >  (Disable)
2. User - >  Network Fault Propagation   >  (Disable)

S - Save
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-10. Fault Propagation Screen

Configuring Date and Time

The Date and Time menu is used to configure the NTP client parameters. The NTP client is used as a means to receive the date and time from the network. When the NTP server is properly configured and accessible, the device displays the real date and time as was received from the NTP server, instead of the system uptime, which is the default state.

➤ **To configure the NTP client parameters:**

- In the Date and Time menu (Configuration › System › Date and Time), configure the NTP client parameters (*Figure 4-11* and *Table 4-3*).

```
                                LA-210
Configuration > System > Date and Time

1. Date                                    ...(0000-00-00)
2. Time                                    ...(00:00:01)
3. NTP Mode                                >  (Unicast Client)
4. GMT                                     >  (0)
5. NTP Server IP Address                   ...(172.17.163.93)
6. NTP Update Interval (sec)               ...(5)
7. Send Initiated NTP Request

ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-11. Date and Time Menu

Table 4-3. Date and Time Configuration Parameters

Parameter	Possible Values	Remarks
Date		Enter the date in the format **<year>-<month>-<day>**
Time		Enter the time in the fomrat **<hour>:<minutes>:<seconds>**
NTP Mode	Unicast Client Disable	Unicast Client – NTP request is sent to a specific IP address Disable – The NTP functionality is disable **Default: Disable**
GMT	-12 ... 12	Offset from Greenwich Mean Time **Default: 0**
NTP Server IP Address	xxx.xxx.xxx.xxx	**Default: 0.0.0.0**
NTP Update Interval (sec)	0 (disable) 1 ... 4294967295	Time (in seconds) between NTP requests **Default: 0 (disa`ble)**
Send Initiated NTP Request		Sends an NTP request regardless of the NTP update interval

Configuring the Application Mode

LA-210 can be set to operate in Flows or Bridge mode as explained below.

➤ **To specify the application mode:**

1. From the Configuration menu, select **System**.

The System menu appears.

2. To select the application mode, select **Application** and press ‹**Enter**› to toggle between **Flows** and **Bridges**.

   The desired mode is specified.

Configuring Physical Layer Port Parameters

LA-210 is equipped with one or four Fast Ethernet interfaces and up to four SHDSL interfaces. The Fast Ethernet and SHDSL physical level configuration menus are accessed from the Physical Layer menu.

Configuring the Fast Ethernet Port

The following parameters can be configured for the Ethernet ports at the physical level:

- Administrative status
- Autonegotiation
- Flow control
- Maximum advertised capability for autonegotiation procedure
- Data rate and duplex mode (only when autonegotiation is disabled)
- MDIX Auto cross-over.
- OAM (EFM)
- Ingress Rate Limit
- VLAN Tag Ether Type

➤ **To configure the Fast Ethernet port at the physical level:**

1. In the **Ethernet** menu (Configuration › Physical Layer › Ethernet), type ‹**F**› or ‹**B**› to select a Fast Ethernet port.
2. Set the physical layer parameters of the selected port. Refer to *Figure 4-12* and *Table 4-4* for further information.

```
                              LA-210
Configuration > Physical Layer > Ethernet

   Port                          (1)
1. Administrative Status         (Up)
2. Auto Negotiation              (Enable)
3. Flow Control                  (Disable)
4. Max Capability Advertised     (100base - TX Full Duplex)
5. MDIX Auto Cross Over          (Enable)
6. OAM (EFM)                     (Enable)
7. Ingress Rate Limit            (100000)
8. VLAN Tag Ether Type           (8100)


F-Forwards; B-Backwards; S-Save
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-12. Ethernet Port Configuration Screen

Table 4-4. Fast Ethernet Port Configuration Parameters

Parameter	Possible Values	Remarks
Port	1 or 4	The Fast Ethernet port number. **Default: 1**
Administrative Status	Up Down	The Fast Ethernet activation. **Default: Up**
Auto Negotiation	Enable Disable	Enables or disable autonegotiation **Default: Enable**
Flow Control	Enable Disable	Used to configure the default administrative PAUSE mode for this interface. **Default: Disable**
Max Capability Advertised	10baseT Half Duplex 10baseT Full Duplex 100baseTX Half Duplex 100base TX Full Duplex	Specifies the set of capabilities advertised by the local autonegotiation entity. **Default: 100BaseTX full-duplex** ***Note**: This parameter only appears when autonegotiation is enabled.*
Speed & Duplex	10baseT Half Duplex 10baseT Full Duplex 100baseTX Half Duplex 100base TX Full Duplex	The static speed and duplex that the port uses when the autonegotiation is disabled. **Default: 100BaseTX full-duplex** ***Note**: This parameter only appears when autonegotiation is disabled.*
MDIX Auto Cross Over	Enable Disable	Enables and disables Auto Cross Over functionality. **Default: Enable**
OAM (EFM)	Enable Disable	Enables/disables IEEE 802.3ah **Default: Enable**
Ingress Rate Limit	64 – 100000 kbps	Defines the rate limit **Default: 100000 kbps**
VLAN Tag Ether Type	0 – FFFF	Defines the VLAN TAG identifier **Default: 8100**

Configuring the SHDSL Ports

This section explains how to configure the SHDSL ports. You configure line and PCS (physical coding sublayer) parameters separately.

➤ **To configure the line parameters:**

1. In the SHDSL menu (Configuration › Physical Layer › SHDSL), select **Line**.

   The Line parameters appear.

2. Configure the parameters as detailed below and then press <**S**>.

   The parameters are set.

```
                              LA-210
Configuration > Physical Layer > SHDSL > Line

1. Line                                          (1)
2. Administrative Status                         (Up)
3. Wire Mode                                >    (2 Wire)
4. Line probe
5. TC Layer                                      (64-65-octet)
6. Power Backoff                            ...  (0)
7. Current Margin                           >    (0 dB [Disable])
8. Worst Margin                             >    (0 dB [Disable])
9. Loop Attenuation Threshold (dB)[0…127]   ...  (0)
10. SNR Margin Threshold (dB)[0…15]         ...  (0)
>
f-Forward, b-Backward
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-13. SHDSL Line Configuration Screen

Table 4-5. SHDSL Line Configuration Parameters

Parameter	Possible Values	Remarks
Line	1–4	The index of the PME (physical medium entity)
Administrative Status	Up Down	Set the administrative status of the SHDSL PME **Default: Up** ***Note:*** *configurable only if STU is set to Central. The STU parameter is visible in Debug mode only.*
Wire Mode	2 Wire 4 Wire 6 Wire 8 Wire	Wire operation mode for SHDSL lines **Default: 2 Wire** ***Note****: Configurable only if TC Layer is set to ATM*

Parameter	Possible Values	Remarks
Line Probe	Enable Disable	This parameter enables/disables support for Line Probe of units associated with an SHDSL span. **Default: Enable** ***Note:*** *Configurable only if STU is set to Central. configurable only if STU is set to Central. The STU parameter is visible in Debug mode only*
TC Layer	64-65-Octet ATM	Operational mode **Default: 64-65-Octet** ***Note****: Only the first line can be configured to ATM. The remaining lines remain invisible.*
Power Backoff	0–31	Temporarily reducing power while transmitting in order to prevent disturbances due to a magnetic field (in ms). **Default: 0 (Off)**
Current Margin	-10–21 db	Selects the downstream/upstream current condition target SNR margin in dB. Press <**N**> or <**P**> to view the next or the previous screen respectively. **Default: 0 (Disable)** ***Note****: Available only when line probing is enabled.*
Worst Margin	-10–21 db	Selects the downstream/upstream worst-case target SNR margin in dB. To configure the worst margin. Press <**N**> or <**P**> to view the next or the previous screen respectively. **Default: 0 (Disable)** ***Note****: Available only when line probing is enabled.*
Loop Attenuation Threshold (dB)	0–127	Defines the loop attenuation alarm threshold. **Default: 0**
SNR Margin Threshold	0–15	This parameter configures the SNR margin alarm threshold.

➤ **To configure the PCS parameters:**

1. In the SHDSL menu (Configuration › Physical Layer › SHDSL), select **PCS**.

   The PCS parameters appear.

2. Configure the parameters as detailed below and then press <**S**>.

   The parameters are set.

```
                                LA-210
Configuration > Physical Layer > SHDSL > PCS

   PCS                                          (1)
1. Administrative Status                        (Up)
2. OAM (EFM)                                    (Enable)
3. Egress Rate Limit                            (100000)
4. VLAN Tag Ether Type (hex)                    (8100)

>
f-Forward; b-backward
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-14. SHDSL PCS Configuration Screen

Table 4-6. SHDSL PCS Configuration Parameters

Parameter	Possible Values	Remarks
PCS	1–4	Index of SHDSL PCS **Default: 1**
Administrative Status	Up Down	Sets the administrative status **Default: Up**
Lines		Lines that are part of the PSC.
OAM (EFM)	Enable Disable	Single segment (link) OAM according to 802.3ah for remote management and fault indication, including remote loopback and MIB parameters retrieval. **Default: Disable**
Egress Rate Limit	64 – 100000 kbps	Defines the rate limit for all queues together. **Default: 100000**
VLAN Tag Ether Type (hex)	0 – FFFF	Defines the VLAN Tag identifier. **Default: 8100**

Configuring the Application Layer Parameters

Configuring the Internal Bridge

The internal bridge connects the unit's ports. Configure the bridge for it to properly process the VLAN tags to maintain priority of the data flows.

The bridge operates in transparent mode (learning is disabled) or filtered mode (learning and filtering are enabled).

If the application mode is set to **Flows**, the bridge parameters do not show.

➤ **To set the application mode to Bridge:**

- From the System menu (Configuration › System), select **Application** and press **Enter**.

  The application mode is set to **Bridge**. The Bridge menu is available in the Applications menu (Configuration › Applications).

➤ **To configure the internal bridge:**

- In the Bridge menu (Configuration › Applications › Bridge), configure the LA-210 bridge. For further information, refer to *Figure 4-15* and *Table 4-7*.

```
                              LA-210
Configuration > Applications > Bridge

1.  VLAN Mode                              (Aware)
2.  Forwarding Mode                        (Filter)
3.  Aging Time (sec) [300 - 4080]     … (300)
4.  Static MAC Table                    []>
5.  Bridge Port                           >
6.  VLAN Membership                       >

S - Save
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-15. Bridge Screen

Table 4-7. Bridge Parameters

Parameter	Possible Values	Remarks
VLAN Mode	Aware Unaware	Forwarding is based on MAC address only or on VLAN+MAC. • **Aware** – Bridge operates according to 802.1Q • **Unaware** – Operates according to 802.1D. **Default: Unaware**
Forwarding Mode	Filter Transparent	Determines whether the bridge learns MAC addresses. • **Filter** – Learning and filtering are enabled • **Transparent** – No learning is performed. Each packet received is forwarded to all other ports automatically, unless static MAC is used. **Default: Filter**
Aging Time (sec)	300–4080	Aging time for entries in the MAC table. If the aging time elapses, and no frame has been received from the MAC, it is erased from the MAC table. **Default: 300** seconds

Using the Static MAC Table

Static MAC addresses are stored in the MAC table.

➤ To add a static address to the table:

1. In the **Static MAC Table** (Configuration › Applications › Bridge › Static MAC Table), press <**A**>.

   The Static MAC Table screen switches to the Add mode as illustrated in *Figure 4-17*.

2. In Add mode, perform the following:

   - Select **MAC Address**, and enter a new MAC address.
   - Select **VLAN ID**, and choose a VLAN ID for the MAC address, 1-4094.
   - Select **Receive Bridge Port**, and choose the interface that this MAC address is attached to.

```
                              LA-210
Configuration > Applications > Bridge > Static MAC Table

                     MAC address            Receive Bridge port

  1                  11-11-11-11-11-11             1
| 2                  22-22-22-22-22-22             2
v 3                  33-33-33-33-33-33             3
  4                  44-44-44-44-44-44             3
  5                  55-55-55-55-55-55             5

1. MAC address … (11-11-11-11-11-11)

C - Clears the table ; S - Save ; A - Add entry
ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 4-16. Static MAC Table Screen

```
                              LA-210
MAC Table Handling

1. MAC address                  … (00-00-00-00-00-00)
2. Bridge port [1 - N]             (1)

S - Save
ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 4-17. Static MAC Table, Add Mode

➤ **To remove a static address from the table:**

- From the Static MAC Table, select a MAC address that you want to remove and press <R>.

  The MAC address is deleted from the table.

➤ **To clear the MAC table:**

1. In the Static MAC Table, press <C> to clear the table.

   The following message appears: **`Are you sure (Y/N)?`**

2. Press <Y> to confirm deletion of all MAC addresses from the table.

Configuring the Bridge Ports

After you set the general bridge parameters, configure the individual bridge ports as explained below.

➤ **To configure the bridge ports:**

1. From the Bridge Port menu (Configuration› Applications › Bridge › Bridge Port), select a bridge port to be configured.
   - To select a bridge port, select Bridge Port and enter the desired bridge port number according to *Table 4-9*.
2. Configure the LA-210 bridge ports according to *Figure 4-18* and *Table 4-8*.

```
                              LA-210
Configuration > Applications > Bridge > Bridge Port

   Bind To                                    >  (Fast Ethernet 1)

1. Bridge port [1 - 6]                        ...(2)
2. Activation                                 >   (Enable)
3. Ingress filtering                              (Disable)
4. Accept frame type                              (All)
5. Port VID / Stacking VID [1 - 4094]         ...(3)
6. Copy Origin Priority                           (Disable)
7. Default Priority Tag [0-7]                 ...(4)
8. Egress Tag Handling                        >  (None)
9. Ingress Tag Handling                       >  (None)

F-Forward; B-Backward; S - Save
ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 4-18. Bridge Ports Screen

Table 4-8. Bridge Port Parameters

Parameter	Possible Values	Remarks
Bridge Port Number	1–6	To switch to the desired bridge port, enter the bridge port number associated with that bridge port. **Default: 2** ***Note:*** • *Bridge port number 1 is reserved for the host bridge port.* • *Available bridge ports depend on the number of Ethernet ports on your LA-210 unit. You cannot add or delete bridge ports.*
Activation	Enable Disable	Specifies if this port is part of the bridge or not. **Default: Enable**
Ingress Filtering	Enable Disable	When Enabled, the device discards incoming frames for VLANs which do not include this port in its member set. When Disabled, the port accepts all incoming frames. **Default: Disable** ***Note**: Available only if the bridge operates in VLAN-Aware mode.*
Accept Frame Type	All Tag Only	**Tag Only** specifies that the device discards untagged frames. **All** specifies that untagged frames received on this port are accepted and assigned to the PVID for this port. **Default: All** ***Note**: Available only if the bridge operates in VLAN-Aware mode.*
Port VID / Stacking VID	1–4094	This is the PVID, the VLAN ID assigned to untagged frames or priority-tagged frames received on this port. If Stacking is enabled, this is the tag to be added. **Default: 2**
Copy Original Priority	Enable Disable	Copy priority from original frame, when stacking an additional tag **Default: Disable**
Default Priority Tag	0–7	Default VLAN frame priority. Applies to untagged frames or stacked tags, when the Copy Original Priority function is disabled. **Default: 0**
Egress Tag Handling	Stacking Stripping None	Stacking: Adds the PVID to every frame transmitted from the port. Stripping: Removes the first VLAN tag from every transmitted frame, on the egress of the port. **Default: None**
Ingress Tag Handling	Stacking Stripping None	Stacking: Adds the PVID to every frame received on the ingress of the port. Stripping: Removes the first VLAN tag from every received frame, on the ingress of the port. **Default: None**

Binding a Bridge Port

The unit is supplied with the bridge ports pre-bound to the physical interfaces as shown in *Table 4-9*.

Table 4-9. Bridge Port Bindings

Bridge Port	Bound to
1	Reserved for management host
2	Fast Ethernet Port 1
3	Fast Ethernet Port 2
4	Fast Ethernet Port 3
5	Fast Ethernet Port 4
6	PCS Port 1

Configuring VLAN Membership

➤ To configure VLAN Membership:

- From the VLAN Membership menu (Configuration › Applications › Bridge › VLAN Membership), perform the following
  - Select **VLAN ID** and type the VLAN ID that you wish to configure.
  - Select **Egress Tagged Ports** and define the set of ports to transmit packets for this VLAN as tagged.
  - Select **Egress Untagged Ports** and define the set of ports to transmit packets for this VLAN as untagged.
  - Press ‹**A**› to add BP to this VLAN.
  - Press ‹**F**› to toggle through the VLAN IDs.
  - Press ‹**R**› to delete the configuration.

```
                              LA-210
Configuration > Applications > Bridge > VLAN Membership

1. VLAN ID                          (1)
2. Egress Tagged Ports            > (1,2)
3. Egress Untagged Ports          > (3,4)

F - Forwards; B - Backwards; R - Remove; S - Save
ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 4-19. VLAN Membership Screen

Configuring Quality of Service (QoS)

Three methods of traffic classification are supported:

- 802.1 priority mapping
- DSCP priority mapping, using tag values
- Priority mapping per bridge port.
- Queue profiles

The classification method is chosen using the Priority Classification menu.

Four traffic queues are supported, which can be assigned priorities using the Priority Mapping menu.

Class 0 (default) has the lowest priority and Class 3 has the highest priority. These queues are priority queues, that is, packets arriving with lower priority will only be transmitted after all packets with higher priority have been transmitted. It implies possible starvation of the lower priority traffic in case the higher priority traffic uses all of the available bandwidth.

Selecting a Traffic Classification Method

➤ To select a traffic classification method:

- From the QoS (Configuration > Applications > QoS) menu, select Priority Classification and choose the desired traffic classification method:
  - 802.1p
  - DSCP
  - Per Port.

```
                              LA-210
Configuration > Applications > QoS

1. Priority Classification                    (802.1p)
2. Priority Mapping                        >
3. Queue Profiles                          >

ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-20. QoS Screen

```
                              LA-210
Configuration > Applications > QoS > Priority Classification

1. 802.1p
2. DSCP
3. Per Port

ESC-Previous menu; !-Main menu; &-Exit;
```

Figure 4-21. QoS Priority Classification Screen

Assigning Priorities to Traffic Queues for 802.1p

➤ To assign priorities to traffic queues for 802.1p:

1. Select **802.1p** as the desired traffic classification method.
2. From the Priority Mapping (802.1p) menu (Configuration › Applications › QoS › Priority Mapping (802.1p)), select the desired priority (0–7) and enter the assigned traffic queue number (0–3). Each traffic queue can be assigned to more than one priority.
3. Repeat the above step for all priorities.

```
                              LA-210
Configuration > Applications > QoS > Priority Mapping (802.1p)

1. User Priority 0 > (Traffic Class 0)
2. User Priority 1 > (Traffic Class 0)
3. User Priority 2 > (Traffic Class 1)
4. User Priority 3 > (Traffic Class 1)
5. User Priority 4 > (Traffic Class 2)
6. User Priority 5 > (Traffic Class 2)
7. User Priority 6 > (Traffic Class 2)
8. User Priority 7 > (Traffic Class 2)

ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-22. Priority Mapping Screen (802.1p)

Assigning Priorities to Traffic Queues for DSCP

➤ To assign priorities to traffic queues for DSCP:

1. Select **DSCP** as the desired traffic classification method.
2. From the Priority Mapping (DSCP) menu (Configuration › Applications › QoS › Priority Mapping (DSCP)), select the desired tag value (0–63) and enter the assigned traffic queue number (0–3). Each traffic queue can be assigned to more than one tag. To add a new entry, press‹**A**› and then enter the tag value and traffic queue number.
3. Repeat the above step for all tag values you wish to change.
4. Press ‹**A**› (Add) to add tag values.

5. Press <R> (Remove) to remove tag values.
6. Press <C> (Copy) to copy tag values.

```
                              LA-210
Configuration > Applications > QoS > Priority Mapping (DSCP)

1. Tag Value 0 > (Traffic Class 0)
2. Tag Value 1 > (Traffic Class 0)
3. Tag Value 2 > (Traffic Class 0)
4. Tag Value 3 > (Traffic Class 0)
..
64. Tag Value 63 > (Traffic Class 0)

A – add; R – Remove ; C - copy
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-23. Priority Mapping Screen (DSCP)

Assigning Priorities to Traffic Queues Per Bridge Port

➤ To assign priorities to traffic queues per bridge port:

1. Select **Per Port** as the desired traffic classification method.
2. From the Priority Mapping (Per Port) (Configuration › Applications › QoS › Priority Mapping (Per Port)) menu, select the desired bridge port.
3. Select **Traffic Class** and enter the traffic queue number (0–3) to be assigned to the bridge port. Each traffic queue can be assigned to more than one port.
4. Repeat the above step for all active bridge ports.

```
                              LA-210
Configuration > Applications > QoS > Priority Mapping (Per
Port)

Bridge Port 1              > (1)
1. Traffic Class           > (Traffic Class 0)

F – Forwards; B – Backwards; C - copy
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-24. Priority Mapping Screen (Per Port)

Configuring Queue Profiles

In order to facilitate congestion management, you are able to sort traffic by applying one queue profile per network or user port and up to 5 queue profiles per LA-210 unit. LA-210 provides five pre-configured queue profiles that you may reconfigure. You cannot add or remove queue profiles.

➤ To define a queue profile:

1. From the QoS menu (Configuration › Application › QoS), select **Queue Profiles**.

   The Queue Profiles menu appears as illustrated in *Figure 4-25*.

```
                                LA-210
Configuration > Applications > QoS > Queue Profiles

   ID                                          (1)
   Queue Default Profile                       (QDefaultProfile)
1. Internal Queues                          >

f - Forward, b - Backward
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-25. Queue Profiles Screen

2. Press <F> or <B>to navigate to the desired queue profile.
3. To configure the current queue profile, select **Internal Queues**.

   The Internal Queues menu appears as illustrated in *Figure 4-26*.
4. Configure the parameters as explained in *Table 4-10*.

```
                                LA-210
Configuration > Applications > QoS > Internal Queues

   Internal Queue                              (1)
1. Scheduling                                  (WFQ)
2. Weight                                      (50)
3. Egress Rate Limit (Kbps)                    (100000)


ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-26. Internal Queues Screen

Table 4-10. Internal Queue Parameters

Parameter	Function	Values
Scheduling	Defines the queue scheduling method. Currently, if one of the internal queues is configured to the WFQ mode, the queues with the higher priority cannot be configured to the strict mode. ***Note**: In configurations with Strict and WFQ queues, the WFQ frames are transmitted only after the transmission of frames associated with the Strict queues is completed.*	**Strict –** High-priority queues that are always serviced first. If a lower-priority queue is being serviced and a packet enters a higher queue, that queue is serviced immediately. **WFQ** – Weighted Fair Queuing, if one port does not transmit, its unused bandwidth is shared by the 'transmitting' queues according to the assigned weight. **Default: Strict**
Weight	Determines the weight of an internal queue when the scheduling weight is configured to WFQ. ***Note**: This parameter does not show if Scheduling is set to Strict.*	**1–100** **Default: 50**
Egress Rate Limit	Defines the rate limit for all queues together.	**0 –100,000** bytes **Default: 100,000**

Configuring the Flows

This section explains how to select the flow interfaces and add packets to the flows according to specific criteria such as the VLAN they belong to. If LA-210's application mode is set to **Bridge**, the Flows parameter does not show.

➤ **To set the application mode to Flows:**

- From the System menu (Configuration › System), select **Application** and press **Enter**.

  The application mode is set to **Flows**. The Flows menu is available in the Applications menu (Configuration › Applications).

➤ **To define the flow interfaces:**

1. From the Flows menu (Configuration › Applications › Flows), select **Flow Interface**.

   The Flow Interface menu appears.

2. Specify the port where the flow starts and the flow key as detailed below.

```
                              LA-210
Configuration > Applications > Flows > Flow Interfaces

   Interface ID[1 - 5]                          (1)
   Port                                      > (ETH-1)
1. Flow Key                                  > (CE-VLAN ID)
2. Defaults                                  >

ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-27. Flows Interfaces Screen

Table 4-11. Flow Interfaces

Parameter	Possible Values	Remarks
Flow Key	• CE-VLAN ID (flow will be based on list of CE-VLANs), • CE -802.1p (flow will be based on a list of CE-VLAN P-bit values) • DSCP (flow will be base on a list of DSCP values) diffServ, IP Precedence (flow will be base on TOS Precedence bits (TOS0-2) • IP Precedence • SP-VLAN ID (flow will be based on list of SP-VLANs) • SP-VLAN ID + SP-802.1p (flow will be based on a list of SP-VLAN ID and SP-VLAN P-bit values)	Determines the field used by the classifier for mapping. **Default:** **User port = CE-VLAN ID** **Network Port = SP-VLAN ID**
Defaults		Refer to *Figure 4-28* and *Table 4-12*

➤ **To define the defaults:**

1. From the Flows Interfaces menu, select **Defaults**.

   The Defaults menu appears.

2. Define the defaults as detailed below.

```
                              LA-210
Configuration > Applications > Flows > Flow Interfaces >
Defaults

1. VLAN ID [1 - 4094]                          (1)
2. 802.1p [0 - 7]                              (0)
3. DSCP [0 - 63]                               (0)
4. IP Precedence [0 - 7]                       (0)

s-Save
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-28. Flows Interface Defaults Screen

Table 4-12. Flow Interface Defaults

Parameter	Possible Values	Remarks
VLAN ID	1 – 4094	Default VLAN Identifier used for mapping purpose when the flow key is SP-VLAN / SP-VLAN And 802.1p / CE-VLAN ID and frames arriving without VLAN tag.
802.1p	0 – 7	Default 802.1p value used for classification purposes when the flow key is CE -802.1p and a frame arrives without VLAN TAG - Or - Used for CoS mapping with the Ingress Priority Method set to 802.1p and a frame arriving without VLAN tag
DSCP	0 – 63	Default DSCP value, used for mapping when the flow key is DSCP and a frame arrives without IP Header - Or - Used for CoS mapping when the Ingress Priority Method = DSCP and a frame arrives without IP header.
IP Precedence	0 – 7	Default IP Precedence value used for mapping purpose when the flow key is IP Precedence and a frame arrives without IP Header – Or – used for CoS mapping when the Ingress Priority Method = IP Precedence and a frame arrives without IP header

➤ **To define the flow:**

1. From the Flows menu (Configuration > Applications > Flows), select **Flow Definition**.

   The Flow Definition menu appears.

2. To add a flow, press <**A**>.

   A new flow is added and a Flow ID is assigned.

3. Specify the desired interface (**ID**) before you press <**S**> for **Save**.

   The interface parameter becomes read-only once you saved for the first time.

4. To assign a flow name, select **Flow Name**, type a name of your choice, and then press <**Enter**>.

   The desired name is assigned to the flow you added.

5. Configure the remaining parameters as detailed below.

   - To navigate to a different flow ID, press <**F**> or <**B**> to browse the Flow IDs forward or backward respectively.
   - To navigate to a different flow interface, press <**^F**> or <**^B**> to navigate forward or backward to the desired flow interface.

```
                                LA-210
Configuration > Applications > Flows > Flow Definition

1. ID [1 - 8]                                ... (1)
2. Name                                      ... (Name)
   Interface                                     ()
3. User Port Mapping Mode                        (User Mapping)
4. Classification                              >
5. CoS Method                                    (Fixed)
6. CoS Value[0-7]                                (1)
7. CoS Profile                                   (CoSDefaultProfile1)
8. Ingress BW Profile                            (Default BW1)
9. Encapsulation                               >
10.CoS                                         >

a-Add; f-Forward; b-Backward; d-Delete; ^F-Frw(Port); ^B-Bkw(Port)
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-29. Flows Definitions Screen

Table 4-13. Flow Definitions

Parameter	Possible Values	Remarks
ID	1 – 8	Flow ID, automatically assigned when adding a flow.
Name		Assign a name to a specific flow **Default: Name-<ID#>**
Interface	ETH-1 – ETH-4 PCS 1	The user interface in which the flow starts. **Default: ETH-1**
User Port Mapping Mode	Unclassified User Mapping	Determines if the flow is composed of user defined ranges or from unclassified frames. **Default: User Mapping**
Classification		Refer to *Figure 4-30* and *Table 4-14*
CoS Method	Fixed Profile	Defines the method to classify frames to specific services. **Default: Profile**
CoS Value	0 – 7	Fixed service CoS value **Default: 0**
CoS Profile		The name of the CoS profile **Default: CoSDefaultProfile1**
Ingress Bandwidth Profile	Unfined DefaultIngressBW1	Ingress Bandwidth Profile name **Default: Undefined**
Encapsulation		Refer to *Figure 4-31* and *Table 4-15*
CoS		Refer to *Figure 4-1* and *Table 4-16*

Classifying the Flows

This section illustrates how to map packets belonging to various logical groups to flows.

➤ To classify (map) packets to flows:

1. From the Flow Definition menu (Configuration > Applications > Flows > Flow Definition), select **Classification**.

   The Classification menu appears.

2. Map the various member IDs to the current flow as detailed below.

```
                              LA-210
Configuration > Applications > Flows > Flow Definition >
Classification

1. VLAN ID Members                        ... (1)
2. VLAN ID 802.1p                         ... (0)
3. DSCP Members                           ... (0)
4. IP Precedence Members                  ... (0)

s-Save
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-30. Flows Definition - Classification Screen

Table 4-14. Flows Definition - Classification

Parameter	Possible Values	Remarks
VLAN ID Members	1 – <highest VLAN ID assigned (max. 4094)>	Defines the members of a VLAN to be mapped to the flow. **Default: No members**
VLAN 802.1p Members	0 - <highest VLAN priority value (max. 7)>	Defines the members of a VLAN P-bit to be mapped to the flow. **Default: No members**
DSCP Members	0 – 64	Defines the members of a DSCP/TOS priority bit to be mapped to the flow. **Default: No members**
IP Precedence Members	0 – 7	Defines the members of an IP Precedence to be mapped to the flow. The IP precedence is derived from the TOS bits 0-2 precedence. **Default: No members**

Encapsulating Packets in the Flows

This section explains how to encapsulate packets in the flows.

➤ To encapsulate packets into flows:

1. From the Flow Definition menu (Configuration > Applications > Flows > Flow Definition), select **Encapsulation**.

   The Encapsulation menu appears.

2. Define the VLAN actions and the Marking methods as follows.

```
                                LA-210
Configuration > Applications > Flows > Flow Definition >
Encapsulation

                                        ()
1. SP-VLAN Action                  >    (Stack)
2. SP-VLAN[1 - 4094]               ...  (0)
3. Marking                              (Profile)
4. Marking Value                   >    (0)
5. CE-VLAN Action                  >    (Preserve)


ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-31. Flows Definition - Encapsulation

Table 4-15. Flows Definition - Encapsulation

Parameter	Possible Values	Remarks
SP-VLAN Action	None Stack	Defines the SP-VLAN action for the current flow. **Default: Stack** ***Note:*** *This parameter displays for UNI ports only.*
SP-VLAN	0, 1 – 4094	The VLAN that will be added to the flow when it egresses from the network. **Default: 0 (no VLAN specified)** ***Note:*** *This parameter displays for UNI ports only.*
Marking	Fixed Profile	The method defined for marking, either using an encoding table defined per flow or using a fixed value. Fixed - Fixed priority value will be marked on SP-TAG. Profile - Marking will be derived from the marking profile attached to the Flow–MIB value 255. ***Note:*** *This parameter displays for UNI ports only.*
Marking Value	1 – 8	An index to the Marking profile. **Default: 1**
CE-VLAN Action	Preserve Update	Defines the CE VLAN action for the current flow. **Default: Preserve** ***Note:*** *This parameter appears for UNI ports only..*

Configuring the Class of Service

This section instructs you on defining a class of service for a flow.

➤ To define a class of service (CoS):

1. From the Flow Definition menu (Configuration > Applications > Flows > Flow Definition), select **CoS**.

   The CoS menu appears.

2. Define the services as detailed below.

```
                              LA-210
Configuration > Applications > Flows > Flow Definition > CoS

                                        (Flow 1 UNI ETH-1)
1. ID [0 - 7]                    >      (0)
2. Name                          ...    (Name string)
3. Ingress BW Profile                   (DefaultBW1)


ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-32. Flows Definition - CoS

Table 4-16. Flows Definition - CoS

Parameter	Possible Values	Remarks
ID	0 – 7	The service associated with the flow displayed at the top of the menu. ***Note:*** *This parameter displays for UNI ports only.*
Name	Name string	A name assigned to the service.
Ingress BW Profile	0, 1 – 8	Ingress bandwidth profile. 0 means no profile specified.

Configuring the OAM

LA-210 provides operation, administration, and maintenance (OAM) in packet-switched networks.

➤ To access the OAM menu:

1. From the **OAM (**Configuration › Applications › OAM) menu, select **End-To-End**.

   OAM options appear listed.

```
                              LA-210
Configuration > Applications > OAM > End-To-End

1. MD Names
2. Standard OAM MAC Address          ... (0180C2000030)
3. Standard OAM EtherType[0 - ffff] ... (8902)
4. Flows

ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-33. End-To-End Menu

Table 4-17. End-To-End Menu

Parameter	Possible Values	Remarks
MD Names		Maintenance Entity Group ID's domain name.
Standard OAM MAC Address		Specifies the MAC Address for Operation and Maintenance. **Default: 0180C2000030**
Standard OAM EtherType	0 - ffff	Specifies the Operation and Maintenance EtherType. **Default: 8902**
Flows		Ethernet Virtual Connections.

2. If necessary, modify the OAM MAC Address and/or the Standard OAM Ether Type.
3. Click **Save**.

Configuring a Maintenance Domain

LA-210 lets you add or remove maintenance domains (MDs) as explained below.

➤ **To view and edit existing MDs:**

1. To view configured MDs, press ‹**F**› or ‹**B**› to scroll forward or backward respectively.

   The associated MD ID, the MD format and the MD name appear.

2. Modify the MD format and the MD name as desired.
3. Select **Save**.

➤ **To add a maintenance domain (MD):**

1. From the End-to-End menu, select **MD Names**.
2. Press ‹**A**›.

   The new MD ID appears as illustrated in *Figure 4-34* and you are able to choose the MD format and assign an MD name as outlined in *Table 4-18*.

```
                                LA-210
Configuration > Applications > OAM > End-To-End > MD Names

   MD ID                                ... (2)
1. MD Format                            >   (String)
2. MD Name                              ... (None)

A-Add New MD  ; F-Forward ; B-Backward ; D-Delete
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-34. MD Names Menu

Table 4-18. MD Names Menu

Parameter	Possible Values	Remarks
MD ID		The maintenance domain's ID
MD Format	None String DNS Like MAC + UINT	Indicates maintenance group entity ID's (MEG ID) domain name format. **Default: String**
MD Name		Indicates maintenance group entity ID's (MEG ID) domain name. One MD name (**None**) remains by default. **Default: The latest configured name or none**

➤ **To delete an MD:**

- To delete an MD, press ‹**D**›.

Configuring a Flow

LA-210 lets you add or remove flows.

Note *In some cases, the user interface may refer to flows also as EVCs.*

➤ **To view existing flows:**

1. From the **End-To-End** (Configuration › Applications › OAM › End-To-End) menu, select **Flows**.

   Flow options appear listed.

2. To view configured flows, press ‹**F**› to scroll forward or ‹**B**› to scroll backward through the list.

➤ **To add a flow:**

1. To add a flow, press ‹**A**›.

   The new flow appears as illustrated in *Figure 4-35*.

2. Configure the flow parameters as outlined in *Table 4-19.*

3. Click **Save**.

```
                              LA-210
Configuration > Applications > OAM > End-To-End > Flows

   Flow[1 - 8]                        ... (1)
1. Flow Name                           ... (Put your String here)
2. SP VLAN[1 - 4094]                   ... (1)
3. Protocol Type                           (Standard)
4. MAID
5. MEP

A-Add New Flow  ; F-Forward ; B-Backward ; D-Delete
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-35. Lows Menu

Table 4-19. Flows Menu

Parameter	Possible Values	Remarks
Flow	1 – 8	Flow ID
Flow Name		Assign a name to the relevant flow.
SP VLAN	1 – 4094	Specify the VLAN used to send the OAM for the specified Maintenance Entity Group (MEP).
Protocol Type	Proprietary Standard	Proprietary refers to RAD's proprietary OAM protocol. If you choose **Proprietary**, you will have to only configure **MEP**. **Default: Standard**
MAID		Refers to the Maintenance Association ID. This parameter only shows if Protocol Type is set to **Standard**.
MEP		Refers to the Maintenance Entity Group End Point.

➤ **To configure the maintenance association's ID (MAID):**

1. Select **MAID**.

   The MAID menu appears as illustrated in *Figure 4-36*.

2. Configure MAID as outlined in *Table 4-20*.
3. Click **Save**.

```
                              LA-210
Configuration > Applications > OAM > End-To-End > Flows > MAID

   Flow ID                          ... (Put your string here)
1. MD ID[1 - 64]                    ... (1)
   MD Format                         >  (None)
   MD Name                              (None)
2. MA Format                         >  (String)
3. MA Name                          ... ()

ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-36. MAID Menu

Table 4-20. MAID Menu

Parameter	Possible Values	Remarks
Flow ID		Displays the Flow ID.
Flow ID	1 - 64	Select the ID of the desired maintenance domain (MD ID)
MD Format		Displays the selected maintenance domain's format (MD Format)
MD Name		Displays the name assigned to the selected maintenance domain (MD Name).
MA Format	String Primary Vlan Unsigned Int 16 ICC	Select the maintenance association's format (MA Format). **Default: String**
MA Name		Assign a name to the maintenance association (MA Name). **Default name: DEFAULT** (in string format only)

➤ **To configure the maintenance entity group's end point (MEP)**

1. Select **MEP**.

   The MEP menu appears as illustrated in *Figure 4-37*.

2. Configure MEP as outlined in *Table 4-21*.

3. Select **Save**.

```
                                LA-210
Configuration > Applications > OAM > End-To-End > Flows > MEP

   Flow ID                              ... (Put your string here)
1. Local ID[0 - 8191]                   ... (0)
2. OAM Destination Address Type             (Multicast)
3. Remote ID                            >   (-)
4. MD Level[0 - 7]                      ... (3)
5. OAM Mode                             >   (Disable)
6. Continuity Verification Mode         >   (CC Based)
7. OAM Destination MAC Address          >   (0120D2000103)
8. Default CC Priority                  >   (0)
9. CC Interval                          >   (1 Second)
10. Services

ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-37. MEP Menu

Table 4-21. MEP Menu

Parameter	Possible Values	Remarks
Flow ID		Displays the Flow ID.
Local ID	0 - 8191	Indicates the maintenance entity group's end point. **Default: 1**
OAM Destination Address Type	Multicast Unicast	Determines the MAC address sent in OAM messages, which may be either RADs proprietary multicast address or a user defined unicast address. **Default: Multicast**
Remote ID	0 – 8191	The Remote MEP ID is the ID that incoming OAM messages will be identified by. Every unit's ID must remain unique. The local and remote ID must therefore not be identical.
MD Level	0 - 7	OAM domain level **Default: 3** ***Note:*** *Read-only in Proprietary mode*
OAM Mode	Disabled Initiate React	Determines the OAM behavior. Disabled: No CC performed, Initiate: The unit will initiate and respond to OAM messages, React: The unit will respond to OAM messages, but not initiate them.

Parameter	Possible Values	Remarks
		Default: Disabled
Continuity Verification Mode	Disabled LB Based CC Based	Determines the CC behavior, visible only in RAD proprietary mode. **Default: Disabled** ***Note**: This parameter is available in Initiate/React OAM mode.*
OAM Destination MAC Address	Unicast Mac Address	Determines the MAC address sent in OAM messages, configurable only for Unicast MAC Address. **Default: 0120D2000100 + MD Level in RAD Proprietary, Standard OAM MAC Address + MD Level in Standard.**
CC Interval	100ms 1 sec 10 sec 1 min 10 min	Sets the CC interval between messages, read-only in RAD proprietary mode. **Default: 1 sec**
Default CC Priority		The priority CFM messages will be sent if no service is defined on the flow. If a service is defined, the CC will be performed at the highest priority service on the flow.
Services		Refer to *Figure 4-38* and *Table 4-22*, visible only in RAD proprietary mode.

➤ **To configure the Services:**

1. From the MEP menu (Configuration › Applications › OAM › End-To-End › Flows › MEP), select **Services**.

   The Services menu appears.

2. Configure the parameters as detailed below and then select **Save**.

```
                              LA-210
Configuration > Applications > OAM > End-To-End > Flows > MEP >
Services

   Service                                  ... (1)
1. Performance Monitoring                   ... (Enabled)
2. Priority                                 ... (0)
3. Delay Objective                          ... (0)
4. Delay Variation Objective                ... (0)

   Event Reporting
5. Frame Loss Ratio                            >
6. Frames Above Delay                          >
7. Frames Above Delay Variation                >
8. Unavailability Ratio                        >
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-38. Service Menu

Table 4-22. Service Menu

Parameter	Possible Values	Remarks
Service	1 – 3	Three services will be automatically created on each defined flow.
Performance Monitoring	Enabled Disabled	Enables/disables Performance Monitoring **Default: Disabled**
Priority	0 – 7	Determines the P bit value sent inside this OAM message that originates from this service. **Default: 0**
Delay Objective	1 – 1000	Determines the delay objective for the specified service. **Default: 0**
Delay Variation Objective	1 – 1000	Determines the delay variation objective for the specified service **Default: 0**
Frame Loss Ratio		Refer to *Figure 4-39* and *Table 4-23*
Frames Above Delay		Refer to *Figure 4-40* and *Table 4-24*
Frames Above Delay Variation		Refer to *Figure 4-41* and *Table 4-25*
Unavailability Ratio		Refer to *Figure 4-42* and *Table 4-26*

```
                              LA-210
Configuration > Applications > OAM > End To End > Flows >
Services > Frame Loss Ratio

1. Rising Threshold            ... (0)
2. Falling Threshold           ... (0)
3. Event Reporting Type        ... (Log)

Please select item <1 to 1>
ESC-prev.menu; !-main menu; &-exit
```

Figure 4-39. Frame Loss Ratio Menu Screen

Table 4-23. Frame Loss Ratio Menu

Parameter	Possible Values	Remarks
Rising Threshold	1 – 4294967296 For Unavailability Ratio / Frame Loss Ratio, the values are: 1E-3,1E-4,1E-5, 1E-6,1E-7,1E-8,1E-9,1E-10	A value above this threshold within the sampling interval for the specified counter will be considered a rising event. **Default: 1**
Falling Threshold	1 – 4294967296 For Unavailability Ratio / Frame Loss Ratio, the values are: 1E-3,1E-4,1E-5, 1E-6,1E-7,1E-8,1E-9,1E-10	A value above this threshold within the sampling interval for the specified counter will be considered a falling event. **Default: 1**
Event Reporting Type	None Log SNMP Trap Trap and Log	The Event type sent out after passing the threshold. **Default: Log**

```
                              LA-210
Configuration > Applications > OAM > End To End > Flows >
Services > Frames Above Delay

1. Rising Threshold            ... (0)
2. Falling Threshold           ... (0)
3. Sampling Interval           ... (0)
4. Event Reporting Type        ... (Trap and Log)

Please select item <1 to 1>
ESC-prev.menu; !-main menu; &-exit
```

Figure 4-40. Frames Above Delay Menu Screen

Table 4-24. Frames Above Delay Menu

Parameter	Possible Values	Remarks
Rising Threshold	1 – 4294967296 For Unavailability Ratio / Frame Loss Ratio, the values are: 1E-3,1E-4,1E-5, 1E-6,1E-7,1E-8,1E-9,1E-10	A value above this threshold within the sampling interval for the specified counter will be considered a rising event. **Default: 1**
Falling Threshold	1 – 4294967296 For Unavailability Ratio / Frame Loss Ratio, the values are: 1E-3,1E-4,1E-5, 1E-6,1E-7,1E-8,1E-9,1E-10	A value above this threshold within the sampling interval for the specified counter will be considered a falling event. **Default: 1**
Sampling Interval	1 – 4294967296	The interval in seconds above which the data is sampled and compared with the rising and falling thresholds.
Event Reporting Type	None Log SNMP Trap Trap and Log	The Event type sent out after passing the threshold. **Default: Trap and Log**

```
                              LA-210
Configuration > Applications > OAM > End To End > Flows >
Services > Frames Above Delay

1. Rising Threshold            ... (0)
2. Falling Threshold           ... (0)
3. Sampling Interval           ... (0)
4. Event Reporting Type        ... (Trap)

Please select item <1 to 1>
ESC-prev.menu; !-main menu; &-exit
```

Figure 4-41. Frames Above Delay Variation Menu Screen

Table 4-25. Frames Above Delay Variation Menu

Parameter	Possible Values	Remarks
Rising Threshold	1 – 4294967296 For Unavailability Ratio / Frame Loss Ratio, the values are: 1E-3,1E-4,1E-5, 1E-6,1E-7,1E-8,1E-9,1E-10	A value above this threshold within the sampling interval for the specified counter will be considered a rising event. **Default: 1**
Falling Threshold	1 – 4294967296 For Unavailability Ratio / Frame Loss Ratio, the values are: 1E-3,1E-4,1E-5, 1E-6,1E-7,1E-8,1E-9,1E-10	A value below this threshold within the sampling interval for the specified counter will be considered a falling event. **Default: 1**
Sampling Interval	1 – 4294967296	The interval in seconds above which the data is sampled and compared with the rising and falling thresholds.
Event Reporting Type	None Log SNMP Trap Trap and Log	The Event type sent out after passing the threshold. **Default: Trap**

```
                              LA-210
Configuration > Applications > OAM > End To End > Flows >
Services > Unavailability Ratio

1. Rising Threshold            ... (0)
2. Falling Threshold           ... (0)
3. Event Reporting Type        ... (Trap)

Please select item <1 to 1>
ESC-prev.menu; !-main menu; &-exit
```

Figure 4-42. Unavailability Ratio Menu Screen

Table 4-26. Unavailability Ratio Menu

Parameter	Possible Values	Remarks
Rising Threshold	1 – 4294967296 For Unavailability Ratio / Frame Loss Ratio, the values are: 1E-3,1E-4,1E-5, 1E-6,1E-7,1E-8,1E-9,1E-10	A value above this threshold within the sampling interval for the specified counter will be considered a rising event. **Default: 1**
Falling Threshold	1 – 4294967296 For Unavailability Ratio / Frame Loss Ratio, the values are: 1E-3,1E-4,1E-5, 1E-6,1E-7,1E-8,1E-9,1E-10	A value above this threshold within the sampling interval for the specified counter will be considered a falling event. **Default: 1**
Event Reporting Type	None Log SNMP Trap Trap and Log	The Event type sent out after passing the threshold. **Default: Trap**

4.3 Additional Tasks

Procedures for miscellaneous tasks are provided in this section.

- Displaying the Inventory
- Changing user name and password
- Transferring software and configuration files
- Resetting LA-210.

Displaying the Inventory

The inventory displays a description of the unit, including its hardware revision and power supply type.

Note *The inventory is a wide table with 132 characters. It is best viewed by setting your terminal to 132 character wide display.*

➤ To display the inventory:

- Select Main Menu›Inventory.

  The Inventory table appears as illustrated in *Figure 4-43*. Use the arrow keys to navigate throughout the table.

```
                                    LA-210
Inventory

  ID      Description     Vendor type  Class         Entity name       HWRev
  1001    LA-210 Device                Chassis       LA-210            1.00
  4001    Power Supply                 Power Supply  PS
| 7001    Fast Eth Port 1              Port          FAST 1
v 7002    Fast Eth Port 2              Port          FAST 2
  7003    Fast Eth Port 3              Port          FAST 3
  7004    Fast Eth Port 4              Port          FAST 4
  7005    SHDSL Line 1                 Port          P 1
  7006    SHDSL Line 2                 Port          P 2
  7007    SHDSL Line 3                 Port          P 3
  7008    SHDSL Line 4                 Port          P 4
  7009    RS-232 Control               Port          Control Port
      - > >

 >
```

Figure 4-43. Typical Inventory Screen – Four Ethernet Ports and Serial Connection

Changing User Name and Password

From the **User Level** menu you can change the current user name and password. LA-210 supports two user names and passwords. *Table 4-27* lists the default user settings supplied with the unit.

Table 4-27. Default User Settings

User	User Name	Password
1	su	1234
2	user	1234

➤ **To change the current user name and password:**

1. From the Management menu (Configuration > System > Management), select **Management Access**.

   The Management Access screen appears as illustrated in *Figure 4-5*.

2. Select **User Access**.

   The User Access screen appears as illustrated in *Figure 4-44*.

3. Select **User Level**.

   The User Level screen appears as illustrated in *Figure 4-45*.

4. Select **User Name**, and enter a new user name.

   The user name can be up to eight characters.

5. Select **Old Password**, and enter the current password.

   The default is 1234.

6. Select **New password** and assign a new password of up to eight characters to the new or existing user name.

Note *The password is case-sensitive.*

7. Select **Confirm New Password** to confirm the new password.

   If the new password is incorrect, an **Illegal confirm password** error message appears. Reassign the new password.

```
                                    LA-210
Configuration > System > Management > Management Access > User Access

1. Change password                 >
2. User Info                       [su]>


ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-44. User Access Screen

```
                                    LA-210
Configuration > System > Management > Management Access > User Access >
User Level

1. User name                    … (USER)
2. Old Password                 … (********)
3. New password                 … (********)
4. Confirm new password         … (********)


S - Save
ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-45. Change Password Screen

Viewing Current Users

From the Management Access screen, you are able to get a list of currently defined users.

➤ **To view a list of users:**

From the User Access menu (Configuration › System › Management › Management Access › User Access), select **User Info**.

A list of currently specified users appears as illustrated in *Figure 4-46*.

```
                                    LA-210
Configuration > System > Management > Management Access > User Access > User
Info

    User name     Access Level     Dynamic/Permanent
 1  USER          RO               Permanent
 2  SU            RW               Permanent

ESC-Previous menu; !-Main menu; &-Exit
```

Figure 4-46. User List

Transferring Software and Configuration Files

This section provides procedures for:

- Installing new software releases on the LA-210 unit
- Transferring configuration files.

Two software versions are stored, each of them in one of the two partitions of the flash memory, which also contains a boot program. The software is stored in a compressed format. The active version is decompressed and loaded into the unit's RAM upon power-up. The passive software is kept for backup purposes. If the active software becomes corrupted, you can swap it with the backup. By default, the unit is delivered with active software only.

New software releases are distributed as ***.img** files, which can be downloaded to the LA-210. When starting a download, the current backup is erased and the new software placed in the backup partition. When downloading is complete, the unit checks the integrity of the new software file. If it is correct, the backup and active files are swapped. The new software release becomes active and the former active software becomes the backup. If a failure occurs while downloading, the new version is erased. In this case, only one version is left stored in the flash memory.

Configuration files can be uploaded for storage and backup.

➤ **To transfer files via TFTP:**

- From the TFTP menu (Utilities › File Transfer › TFTP), perform the following.
  - Select **Server IP Address,** and enter the IP address of the TFTP server.
  - Select **Remote File Name**, and enter a file name.
  - Select **File Type**, and choose whether you intend to transfer a software program (IMG) or configuration file.
  - Select **Save** to save the changes.
  - Select **Command** to start the desired procedure:
    - **Upload**: To save a software or configuration file on a remote server
    - **Download**: To transfer a software or configuration file to the unit.

    LA-210 starts file transfer.

    The TFTP file transfer process is logged with the following system messages:

    - TFTP – Starting Upload
    - TFTP – Starting Download
    - TFTP – Upload Failed
    - TFTP – Download Failed.

    Once the image has been successfully uploaded, you are asked to reset the unit to load the new image.

```
                              LA-210
Utilities > File Transfer > TFTP

   Status                          (No operation)
   Error                           (No error)

1. Server IP Address               (0.0.0.0)
2. Remote File name                ()
3. File Type                       (Configuration)
4. Command                       >

ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 4-47. TFTP Screen

Resetting LA-210

This section describes two types of reset functions:

- Resetting configuration parameters to default settings
- Overall reset of the device
- Reset the PCS.

Resetting to the Default Settings

Using the terminal application, you can reset the unit to its default settings.

➤ To reset to the default settings:

1. From the System menu (Configuration › System), select **Factory Defaults**.

   The following message appears:

```
The device will restart with default configuration, proceed?
                              (Y/N)
```

2. Press ‹**Y**› to confirm the reset.

   All parameters are reset to the factory default, and the unit is reset.

Resetting the Unit

You can perform an overall reset of the unit.

➤ To reset LA-210:

1. From the Utilities menu, select **Reset Device**.

   The following confirmation message appears:

```
The device will restart. Do you want to proceed? (Y/N).
```

2. Press ‹**Y**› to confirm the reset.

   The device resets.

Chapter 5

Configuring a Flow-Based Point-To-Point Application

This chapter provides detailed instructions on assembling, configuring and using a flow-based point-to-point application.

The configuration used for the application is illustrated below. It includes a server PC and a client PC, enabling you for example to screen a movie and simultaneously testing the performance at different bandwidths and priorities. Two ETX-202 units represent the termination unit, providing a demarcation point between the LAN and the management and client stations.

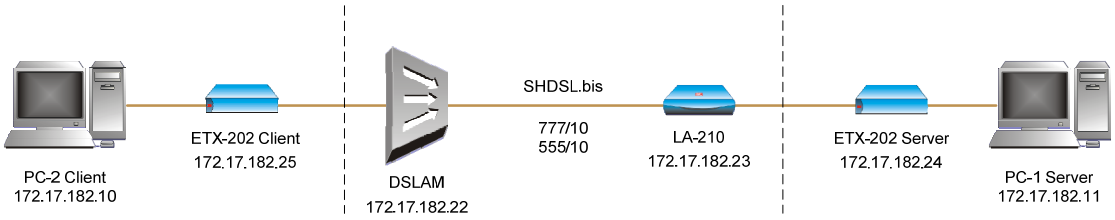


Figure 5-1. Typical Application

5.1 Assembling the Hardware

The section below lists required equipment and instructs you on connecting cables to each unit.

Required Equipment

The hardware configuration requires the following:

- One LA-210 unit
- One DSLAM unit
- Two ETX-202 units (ETX-202 Client and ETX-202 Server)
- Two PCs
- Four Ethernet cables
- One DSL cable.

Connecting Cables

Figure 5-2 illustrates the required cable connections.

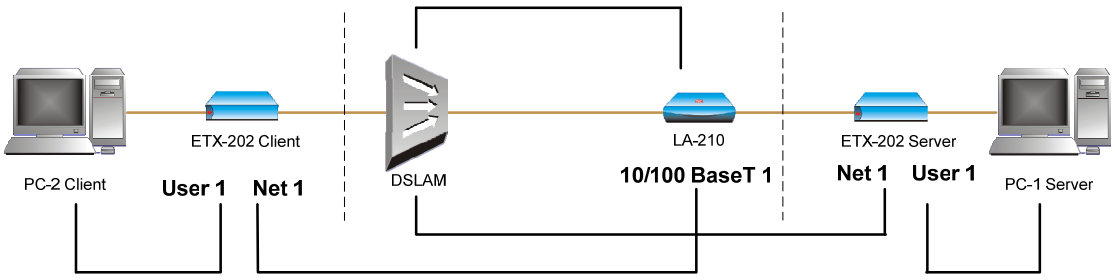


Figure 5-2. Application Setup and Cable Connections

➤ **To connect the units to the PCs and to each other:**

1. Use a network cable to connect **PC-1 Server** and **ETX-202 Server**'s **User Port 1**.
2. Use a network cable to connect **ETX-202 Server's Net Port 1** to the DSLAM.
3. Use a DSL cable to connect the SHDSL.bis port of **LA-210** to the DSLAM.
4. Use a network cable to connect **PC-1 Client** and **ETX-202 Client**'s **User Port 1**.
5. Use a network cable to connect **ETX-202 Client**'s **Net Port 1** to **LA-210's Port 1**.

5.2 Configuring the Units for Basic Applications

Configuration Overview

You must configure the following to deploy LA-210 and ETX-202 units in this application:

- System parameters (host IP, default gateway)
- Flow Interface configuration
- Flows.

Table 5-1. System Configuration Summary

Device	Host IP	IP mask	Default Gateway
LA-210	172.17.182.23	255.255.255.0	172.17.182.1
DSLAM	172.17.182.22	255.255.255.0	172.17.182.1
ETX-202 (Client)	172.17.182.25	255.255.255.0	172.17.182.1
ETX-202 (Server)	172.17.182.24	255.255.255.0	172.17.182.1

Table 5-2. Flow Configuration Summary – LA-210

Flow Interface	Flow ID	CE-VLAN-ID	Flow Interface	SP-VLAN-ID
ETH-1	1	555 777	UNI ETH-1	10

Table 5-3. Configuration Summary – ETX-202 (Client and Server)

Interface	Host Tagging	Host VLAN ID	Port/Stacking VID	Tag Handling
User 1	Tagged	555	555 777	Stack
User 2	Tagged	555	555 777	Stack

Accessing ETX-202 and LA-210 Units

This section instructs you on accessing the LA-210 and ETX-202 units using the terminal application.

➤ **To log on:**

1. Configure the parameters of your terminal application as listed below.
   - Baud rate: **9600**
   - Data bits: **8**
   - Stop bits: **1**
   - Parity: **None**
   - Flow Control: **None**
2. If not already done, connect a serial cable to the respective unit's Control port and your PC's COM port.
3. Press <**Enter**>.

   You are asked for the user name and the password.
4. Enter the user name for Super User and the associated password. The default user name is **su** and the default password is **1234**.

   The respective unit's main menu appears.

Configuring LA-210

Operating LA-210 in flow-based operation mode requires configuring the flow definition and specify VLANs as members of the desired flow.

Before configuring the flow definition, you should first configure the IP settings.

➤ **To configure the IP settings:**

1. Log on to LA-210 as explained under *Accessing ETX-202 and LA-210 Units*.

   The Main menu appears.

2. Navigate to the Host menu and adjust the IP settings as illustrated below.

```
                                LA-210
Configuration>System

 1. IP Address                ... (172.17.182.23)
 2. Mask                      ... (255.255.255.0)
 3. Default Gateway           ... (172.17.182.1)
 4. Read Community            ... (public)
 5. Write Community           ... (private)
 6. Trap Community            ... (public)
 7. Encapsulation             >
>
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-3. Host Menu

➤ **To switch to the Flow mode:**

1. Log on to LA-210 as explained under *Accessing ETX-202 and LA-210 Units.*

   The Main menu appears.

2. In the System menu (Configuration›System), under **Application Mode**, select **Flows Mode**.

   LA-210 is set to flow-based operation.

```
                                LA-210
Configuration>System

 1. Management          >
 2. Terminal            >
 3. Fault Propagation   >
 4. Date and Time       >
 5. Application Mode        (Flows Mode)
 6. Factory Defaults
>
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-4. System Menu

➤ **To add a flow definition:**

1. Navigate to the Flow Definition screen (Configuration›Applications›Flows›Flow Definition)

   The Flow Definition screen appears.

2. Add a flow by pressing ‹**A**›.

   Flow Definition parameters appear.

3. Assign the name **VLAN777-555** to this flow and then press ‹**S**›.

```
                                    LA-210
Configuration>Applications>Flows>Flow Definition

                                (Flow 1 UNI ETH-1)
 1. ID[1 - 8]                ... (1)
 2. Name                     ... (VLAN777-555)
    Interface                    (1)
 3. User port Mapping Mode       (User Mapping)
 4. Classification           >
 5. CoS Method                   (Profile)
 6. CoS profile              >   (CoSDefaultProfile1)
 7. Ingress BW profile       >   (Undefined)
 8. Encapsulation            >
 9. CoS                      >

>
a-Add; f-Forward; b-Backward; d-Delete; ^F-Frw(Port); ^B-Bkw(Port)
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-5. Flow Definition Menu

4. In the Flow Interfaces menu (Configuration›Applications›Flows›Flow Interfaces), verify that the flow is classified according to **CE-VLAN ID**.

```
                                    LA-210
Configuration>Applications>Flows>Flow Interfaces

    Interface ID[1 - 5]                     (1)
    Port                              >     (ETH-1)
 1. Flow Key                          >     (CE-VLAN ID)
 2. Defaults                          >

>
f-Forward; b-Backward
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-6. Flow Interfaces Menu

➤ **To add VLANs as members to the flow.**

1. To define VLAN IDs as members of Flow 1, navigate to **CE VLAN ID Members** (Configuration›Applications›Flows›Flow Definition›Classification›CE VLAN Members).
2. Enter **777** and press ‹**S**› to save your settings.

   VLAN 777 is added as a member to Flow 1.
3. Press ‹**A**› to add an additional member.
4. Enter **555** and press ‹**S**› to save your settings.

   VLAN 555 is added as an additional member to Flow 1.

```
                                    LA-210
Configuration>Applications>Flows>Flow Definition>Classification>CE VLAN ID
Members (555,777)

 1. [1 - 4094]... (555)
 2. [1 - 4094]... (777)
 3. Delete Range...

>

ESC-prev.menu; !-main menu; &-exit; A-add                          1 M/ 1 C
```

Figure 5-7. CE VLAN ID Members Menu

5. Press ‹**ESC**› to return to the Classification screen.

   The Classification screen reflects the new VLAN IDs.

```
                                    LA-210
Configuration>Applications>Flows>Flow Definition>Classification

                                (Flow 1 UNI ETH-1)
 1. CE VLAN ID Members      >    (555,777)

>
ESC-prev.menu; !-main menu; &-exit                                 1 M/ 1 C
```

Figure 5-8. Classification Screen

➤ **To define the SP-VLAN:**

1. In the Encapsulation menu (Configuration›Applications›Flows›Flow Definition›Encapsulation), select **SP-VLAN** and enter **10**.
2. The SP-VLAN 10 is added to the flow on the service provider side.

```
                                    LA-210
Configuration>Applications>Flows>Flow Definition>Encapsulation

                                (Flow 1 UNI ETH-1)
 1. SP-Vlan Action              (Stacking)
 2. SP-VLAN[1 - 4094]      ... (10)
 3. Marking Method              (Profile)
 4. Marking Profile        >    (MarkingDefaultProfile1)
 5. CE-VLAN action         >    (Preserve)

>
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-9. Encapsulation Screen

Configuring ETX-202 Server and Client

In addition to the IP settings, you have to enable Host Tagging and then, configure the VLAN and the bridge port. Except for the IP address, both ETX-202 units are configured with the same parameters.

➤ **To configure the IP settings:**

1. Navigate to the Host menu (Configuration›Management›Host›Encapsulation) and configure the IP settings as illustrated below.

```
                                    ETX-202
Configuration>System>Host

 1. IP Address             ... (172.17.192.25)
 2. IP Mask                ... (255.255.255.0)
 3. Default Gateway        ... (172.17.192.1)
 4. Bind                       (Bridge Port)
 5. DHCP                       (Disable)
 6. Default IP             ... (0.0.0.0)

>
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-10. ETX-202 Client - Host Menu

2. Press ‹**S**› to save the IP settings.

➤ **To configure the VLAN settings:**

1. Navigate to the Encapsulation menu (Configuration›System›Management›Host›Encapsulation).

```
                                ETX-202
Configuration>System>Management>Host>Encapsulation

 1. Host Tagging                              (Tagged)
 2. Host VLAN ID[1 - 4094]                ... (333)
 3. Host VLAN Priority[0 - 7]             ... (7)
 4. Security Definition                   >   (All)

>
Please select item <1 to 4>
ESC-prev.menu; !-main menu; &-exit                                1 M/ 1 C
```

Figure 5-11. ETX-202 Client – Enabling Host Tagging

2. Select Host Tagging.

   Host Tagging toggles to **Enabled**.

3. Press ‹**S**› to save this setting.

➤ **To configure the bridge port:**

1. Navigate to the Bridge Port menu (Configuration›Bridge›Bridge Port).
2. Navigate to **User Port 1** and **User Port 2** and configure the respective parameters as illustrated below.

```
                                ETX-202
Configuration>Bridge>Bridge Port

    Port Label                    >    (3)
    Bridge port                   >    (User 1)
 1. Port\Stacking VID[1 - 4094]    ... (777)
 2. Default Priority Tag [0 - 7]   ... (4)
 3. Tag Handling                       (Stack)

Please select item <1 to 3>
F-Forward
ESC-prev.menu; !-main menu; &- exit                               1 M/ 1 C
```

Figure 5-12. ETX-202 Client User Port 1– Bridge Port Menu

```
                                ETX-202
Configuration>Bridge>Bridge Port

   Port Label                    >    (4)
   Bridge port                   >    (User 2)
 1. Port\Stacking VID[1 - 4094]    ... (555)
 2. Default Priority Tag [0 - 7]   ... (7)
 3. Tag Handling                       (Stack)

Please select item <1 to 3>
F-Forward
ESC-prev.menu; !-main menu; &- exit                                  1 M/ 1 C
```

Figure 5-13. ETX-202 Client User Port 2– Bridge Port Menu

Note *This application allows using ETX-202 Version 3.5 or higher. Depending on the version in use, additional menu items may be visible. Do not modify the associated settings if not instructed otherwise.*

5.3 Configuring the Units for Advanced Configurations

This chapter explains how to map priority bits to classes of service. You can map each p.bit to any CoS, thus setting different priorities via the CoS profile configuration. You also can set a fixed p.bit per flow.
In the current example you will map p.bits to classes of service (CoS) as follows:

- Map p.bit 7 to CoS 6.
- Map p.bit 4 to CoS 3.
- Define two services for each CoS, VLAN 777 with CoS 3 (p.bit 4) and VLAN 555 with CoS 6 (p.bit 7).
  In addition, you can determine the bandwidth options (policer) for each service.
- Map CoS to **Queue**. This mapping is not configurable, but it is possible to set the queue definition to **Strict** or **WFQ**.

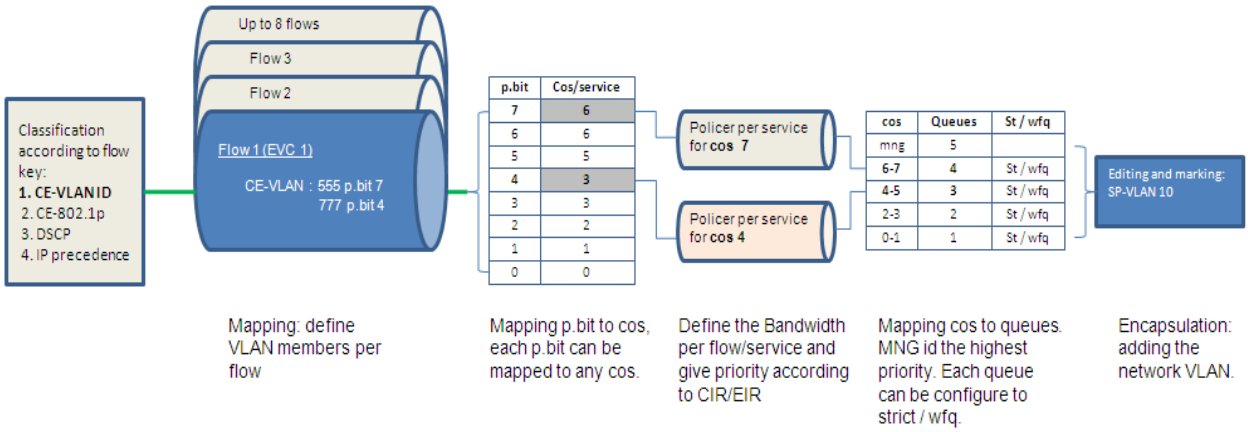

Up to 8 flows
Flow 3
Flow 2
Flow 1 (EVC 1)
CE-VLAN : 555 p.bit 7
777 p.bit 4
Classification according to flow key:
1. CE-VLAN ID
2. CE-802.1p
3. DSCP
4. IP precedence
p.bit
Cos/service
Policer per service for cos 7
Policer per service for cos 4
cos
Queues
St / wfq
mng
Editing and marking: SP-VLAN 10
Mapping: define VLAN members per flow
Mapping p.bit to cos, each p.bit can be mapped to any cos.
Define the Bandwidth per flow/service and give priority according to CIR/EIR
Mapping cos to queues. MNG id the highest priority. Each queue can be configure to strict / wfq.
Encapsulation: adding the network VLAN.

Figure 5-14. Mapping Priority Bits (p.bits) to Classes of Service (CoS) - Scheme

➤ **To map p.bits to CoS:**

1. Navigate to the CoS Profiles menu (Configuration›Applications›QoS›Cos Profiles).

   A default CoS profile with default mapping appears.

```
                                    LA-210
Configuration>Applications>QoS>Cos Profiles

 1. ID[1 - 8]                ... (1)
 2. Name                     ... (CoSDefaultProfile1)
 3. Ingress Priority Method >    (IEEE 802.p)
 4. Mapping                  >
>
a-Add; f-Forward; b-Backward
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-15. CoS Profile

2. Press ‹**A**› to add a new CoS profile.

   A CoS profile with default parameters appears.

3. Assign a name of your choice to the profile, for example **CosProfile_no_1**.

4. Press ‹**S**› to save your settings.

```
                                    LA-210
Configuration>Applications>QoS>Cos Profiles

 1. ID[1 - 8]                ... (2)
 2. Name                     ... (CosProfile_no_1)
 3. Ingress Priority Method >    (IEEE 802.p)
 4. Mapping                  >

>
s-Save
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-16. New CoS Profile

5. Select **Mapping**.

   The Mapping screen appears.

6. Set **Tag (p.bit) 4** to **3** and **Tag (p.bit) 7** to **6**.

```
                                    LA-210
Configuration>Applications>QoS>Cos Profiles>Mapping

 1. Tag 0[0 - 7]    ... (0)
 2. Tag 1[0 - 7]    ... (1)
 3. Tag 2[0 - 7]    ... (2)
 4. Tag 3[0 - 7]    ... (3)
 5. Tag 4[0 - 7]    ... (3)
 6. Tag 5[0 - 7]    ... (5)
 7. Tag 6[0 - 7]    ... (6)
 8. Tag 7[0 - 7]    ... (6)
>
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-17. Mapping p.bits to Flow 1

➤ **To link Flow 1 to the newly created CoS profile:**

1. Navigate to the Flow definition menu (Configuration›Applications›Flows›Flow Definition).

```
                                    LA-210
Configuration>Applications>Flows>Flow Definition

                                (Flow 1 UNI ETH-1)
 1. ID[1 - 8]               ... (1)
 2. Name                    ... (VLAN777-555)
    Interface                   (1)
 3. User port Mapping Mode      (User Mapping)
 4. Classification          >
 5. CoS Method                  (Profile)
 6. CoS profile             >   (CoSDefaultProfile1)
 7. Ingress BW profile      >   (Undefined)
 8. Encapsulation           >
 9. CoS                     >

>
a-Add; f-Forward; b-Backward; d-Delete; ^F-Frw(Port); ^B-Bkw(Port)
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-18. Flow Definition

2. Set the CoS Method parameter to **Profile**.
3. Select **CoS Profile**.

   The existing CoS profiles appear listed.

4. Select the profile you added. The example uses the name **CosProfile_no_1**.

```
                                    LA-210
...>Applications>Flows>Flow Definition>CoS profile  (CoSDefaultProfile1)

 1. CoSDefaultProfile1
 2. CosProfile_no_1

>

ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-19. CoS Profiles

```
                                    LA-210
Configuration>Applications>Flows>Flow Definition

                                (Flow 1 UNI ETH-1)
 1. ID[1 - 8]               ... (1)
 2. Name                    ... (VLAN777-555)
    Interface                   (1)
 3. User Port Mapping Mode      (User Mapping)
 4. Classification          >
 5. CoS Method                  (Profile)
 6. CoS Profile             >   (CosProfile_no_1)
```

```
 7. Ingress BW Profile    >   (Undefined)
 8. Encapsulation         >
 9. CoS                   >

>
a-Add; f-Forward; b-Backward; d-Delete; ^F-Frw(Port); ^B-Bkw(Port)
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-20. Flow Definition

➤ **To define a bandwidth profile for VLAN 777:**

1. Navigate to the Bandwidth Profiles menu (Configuration›Applications›QoS›Bandwidth Profiles)

```
                                  LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                ... (1)
 2. Name                     ... (DefaultIngressBW1)
 3. CIR(Kbps)[0 - 100000]    ... (100000)
 4. CBS(Bytes)[0 - 32000]    ... (12176)
 5. EIR(Kbps)[0 - 100000]    ... (0)
 6. EBS(Bytes)[0 - 32000]    ... (12176)

>
a-Add; f-Forward; b-Backward
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-21. Bandwidth Profile

2. To add a new profile, press ‹**A**›.

```
                                  LA-210
*Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                ... (2)
 2. Name                     ... (Put your string here)
 3. CIR(Kbps)[0 - 100000]    ... (100000)
 4. CBS(Bytes)[0 - 32000]    ... (12176)
 5. EIR(Kbps)[0 - 100000]    ... (0)
 6. EBS(Bytes)[0 - 32000]    ... (12176)

>
s-Save
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-22. Adding a Bandwidth Profile

3. Under **Name**, enter the desired bandwidth profile name, for example **BW_for_service_777**.
4. Set **CIR** to **5000 Kbps** and **EIR** to **2000 Kbps** .

5. Press ‹**S**› to save your settings.

```
                                LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                ... (2)
 2. Name                     ... (BW_for_service_777)
 3. CIR(Kbps)[0 - 100000]    ... (5000)
 4. CBS(Bytes)[0 - 32000]    ... (12176)
 5. EIR(Kbps)[0 - 100000]    ... (2000)
 6. EBS(Bytes)[0 - 32000]    ... (12176)

>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-23. Adding a Bandwidth Profile for VLAN 777

➤ **To define a bandwidth profile for VLAN 555:**

1. Return to the Bandwidth Profiles menu, press ‹**A**›, and then follow the instructions above.
2. Assign a name to the bandwidth profile, for example **BW_for_Service555**.
3. Set **CIR** to 2000 Kbps and **EBS** to 12176 Bytes.
4. Press ‹**S**› to save your settings.

```
                                LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                ... (3)
 2. Name                     ... (BW_for_Service555)
 3. CIR(Kbps)[0 - 100000]    ... (2000)
 4. CBS(Bytes)[0 - 32000]    ... (12176)
 5. EIR(Kbps)[0 - 100000]    ... (1000)
 6. EBS(Bytes)[0 - 32000]    ... (12176)

>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-24. Adding a Bandwidth Profile for VLAN 555

➤ **To define a service for VLAN 777 and CoS 3 (p.bit 4)**

1. Navigate to the CoS menu (Configuration›Applications›Flows›Flow Definition›CoS).

```
                                    LA-210
Configuration>Applications>Flows>Flow Definition>CoS

                            (Flow 1 UNI ETH-1)


>

a-Add
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-25. CoS Screen

1. To add a service, press <**A**>.

   CoS parameters appear.

```
                                    LA-210
*Configuration>Applications>Flows>Flow Definition>CoS

                            (Flow 1 UNI ETH-1)
 1. ID[0 - 7]           ... (3)
 2. Name                ... (Service777_pbit_4)
 3. Ingress BW Profile >    (Undefined)

>
s-Save
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-26. CoS Parameters

2. Select **ID** and enter **3** (cos 3 for p.bit 4), and then press <**Enter**>.
3. Assign a name to the service, for example **Service777_pbit_4**, and then press <**Enter**>.

   The service is added.

➤ **To add an additional service:**

1. In the CoS menu (Configuration›Applications›Flows›Flow Definition›CoS), press <**A**> to add an additional service.
2. Select **ID** and enter 6 (CoS 6 for p.bit 7).
3. Select **Name** and assign a name to the service, for example **Service555_pbit_7**, and then press <**Enter**>.

   The service is added.

```
                                    LA-210
Configuration>Applications>Flows>Flow Definition>CoS

                              (Flow 1 UNI ETH-1)
 1. ID[0 - 7]            ... (3)
 2. Name                 ... (Service555_pbit_7)
 3. Ingress BW Profile >     (Undefined)
>

a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-27. Adding a Service

➤ **To bind a BW profile to Service555_pbit_7:**

1. Press ‹**F**› or ‹**B**› to navigate to **Service555_pbit_7**.
2. In the desired CoS menu, select **Ingress BW Profile**.

   The ingress BW profile CoS appears.

```
                                    LA-210
..>Applications>Flows>Flow Definition>CoS>Ingress BW Profile (Undefined)

 1. Undefined
 2. DefaultIngressBW1
 3. BW_for_Service777
 4. BW_for_Service555

>
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-28. Ingress BW Profiles

3. Select **BW_for_Service555**.

   The BW profile is bound to **Service555_pbit_7** (*Figure 5-29*).
4. Press ‹**S**› to save the settings.

```
                                    LA-210
Configuration>Applications>Flows>Flow Definition>CoS

                              (Flow 1 UNI ETH-1)
 1. ID[0 - 7]            ... (3)
 2. Name                 ... (Service555_pbit_7)
 3. Ingress BW Profile >     (BW_for_service_555)

>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

*Figure 5-29. Ingress BW Profile **BW_for_service_555** bound to **Service555_pbit_7***

➤ **To bind a BW profile to Service777_pbit_4:**

1. Return to the CoS menu and press ‹**F**› or ‹**B**› to navigate to **Service7775_pbit_4**.
2. In the associated CoS menu, select **Ingress BW Profile**.

   The ingress BW profile appears.

```
                                    LA-210
..>Applications>Flows>Flow Definition>CoS>Ingress BW Profile (Undefined)

 1. Undefined
 2. DefaultIngressBW1
 3. BW_for_Service777
 4. BW_for_Service555

>
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-30. Ingress BW Profiles

3. Select **BW_for_Service777**.

   The BW profile is bound to **Service777_pbit_4** (*Figure 5-29*).
4. Press ‹**S**› to save the settings.

```
                                    LA-210
Configuration>Applications>Flows>Flow Definition>CoS

                             (Flow 1 UNI ETH-1)
 1. ID[0 - 7]           ... (3)
 2. Name                ... (Service777_pbit_4)
 3. Ingress BW Profile >    (BW_for_service_777)

>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

*Figure 5-31. Ingress BW Profile **BW_for_service_777** bound to **Service777_pbit_4***

Configuring the DSLAM

The DSLAM configuration has to match the configuration of the LA-210 units with the difference that the clock mode is configured to Central mode.

5.4 Using the Setup to Screen a Movie

You use the two PCs on both sides as server and client. The server (PC1-Server) holds a movie that is going to be viewed from the client side (PC-2 Client). To screen the movie, you use a streaming application, for example the VLC Media Player. For brief instructions on using the VLC Media Player, refer to the section below.

While playing the movie, you may perform various tests outlined in the next chapters.

Using the VLC Media Player

To transmit and play the movie, you may use any streaming application with an associated player on the client side, although this application assumes the use of an already installed VLC Media Player on both the server and the client PCs. A movie that will transmit at around 1.5 Mbps must be available on the server side.

➤ **To start VLC:**

- Double click the VLC.exe short cut

on your desktop.

➤ **To start the PC-1 (Server):**

1. Navigate to **File › Open File...**

   Various tabs with parameters appear.

2. Click the File Tab and, under Advanced Options, select Stream/Save.

   The Settings button becomes available.

3. Click ‹**Settings**›.

   Stream output options become available.

4. Select **RTP** and, under **Address**, enter the multicast address **224.0.0.0** and then click ‹**OK**›.

5. Start the desired movie.

➤ **To connect from the PC-2 (Client):**

1. Navigate to **File › Open File...**

   Various tabs with parameters appear.

2. Click the Network Tab.

3. Select **UDP/RTP Multicast** and define the same multicast address as defined on the server, which is **224.0.0.0** in the current example.

4. Click ‹**OK**›.

5. Start playing the movie.

6. Verify that you can see the movie playing on the client side.

5.5 Testing the Flow Based Configuration

This section instructs you on testing the application you configured.

Ping Tests

In order to test whether all components are properly connected and configured, you may ping from various locations as detailed below.

- Ping from PC-1 Server to PC-2 Client and verify the ping ends successfully.
- Ping from PC-2 Client to PC-1 Server and verify the ping ends successfully.
- Ping from ETX-202 Client to ETX-202-2 Server and verify the ping ends successfully.
- Ping from ETX-202 Server to ETX-202 Client and verify the ping ends successfully.

➤ **To perform a ping test from an ETX-202 unit:**

1. Connect the server PC to the ETX-202 unit that will send the ping via the serial port, start the terminal application and then log on to the ETX-202 unit.

   The Main menu appears.

2. Navigate to the Ping menu (Diagnostics>Ping).

   The Ping menu appears (Figure 5-32).

```
                                ETX-202
Diagnostics>Ping

1. Destination IP Address              ... (172.17.182.24)
2. Number of Frames to Send[0 - 50]    ... (1)
3. Send Ping
4. Stop Ping

>

ESC-prev.menu; !-main menu; &-exit                              1 Mngr/s
```

Figure 5-32. ETX-202 Ping Menu

3. Select **Destination IP Address** and enter the IP address of the ETX-202 unit that you wish to ping.
4. Specify the number of frames (packets) to send.
5. To start pinging the other ETX-202 unit, select **Send Ping**.

   The ping results appear at the bottom of the screen.

Policer Testing

To perform the policer testing, you have to connect the serial port of LA-210 to a PC's COM port with a terminal.

Connect by terminal to LA-210, located on the server side.

The Bandwidth profile of CoS 3 (service 777 p.bit 4) has been previously configured as follows:

```
                                    LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                ... (2)
 2. Name                     ... (BW_for_service_777)
 3. CIR(Kbps)[0 - 100000]    ... (5000)
 4. CBS(Bytes)[0 - 32000]    ... (12176)
 5. EIR(Kbps)[0 - 100000]    ... (2000)
 6. EBS(Bytes)[0 - 32000]    ... (12176)
```

Figure 5-33. Previously configured Bandwidth Profile - CIR = 5 Mbps

CIR is the committed bandwidth that the service provider guarantees to the user, therefore they are called green packets.
EIR means that the service for these frames is not guaranteed and depends on available bandwidth. These packets are called yellow packets.
In the current configuration, you will use EIR = 5 Mbps and EIR = 2 Mbps.

➤ To test the bandwidth profiles:

1. While viewing the movie from the client PC, navigate to Monitoring›Application›Flows›CoS.

   The CoS menu appears, indicating that all packets are green.

```
                                    LA-210
*Monitoring>Application>Flows>CoS

    Flow Name          ... (VLAN777-555)
    Flow ID[1 - 8]     ... (1)               Direction          >   (Upstream)
    Fwd Green Packets      (1288)            Fwd Green bytes        (1795534)
    Fwd Yellow Packets     (0)               Fwd Yellow bytes       (0)
    Dscrd Green Packet     (0)               Dscrd Green bytes      (0)
    Dscrd Yellow Packe     (0)               Dscrd Yellow bytes     (0)
    Dscrd Red Packets      (0)               Dscrd Red bytes        (0)

 1. CoS ID[0 - 7]      ... (3)

f-Forward; b-Backward; c-Clear Statistics
ESC-prev.menu; !-main menu; &-exit                                   1 M/ 1 C
```

Figure 5-34. CoS Statistics - CIR = 5 Mbps, EIR = 2 Mbps

The movie is transmitting at around 1.5 Mbps and CIR = 5 Mbps so all the packets are green and forwarding.

2. Reduce **CIR** to 1000 Kbps (1 Mbps).

```
                                    LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                ... (2)
 2. Name                     ... (BW_for_service_777)
 3. CIR(Kbps)[0 - 100000]    ... (1000)
 4. CBS(Bytes)[0 - 32000]    ... (12176)
 5. EIR(Kbps)[0 - 100000]    ... (2000)
 6. EBS(Bytes)[0 - 32000]    ... (12176)

>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                                   1 M/ 1 C
```

Figure 5-35. Previously configured Bandwidth Profile - CIR = 1 Mbps, EIR = 2 Mbps

3. While playing the movie, navigate to Monitoring›Application›Flows›CoS.

Green (CIR) and yellow (EIR) packets are now forwarded.

```
                                    LA-210
*Monitoring>Application>Flows>CoS

    Flow Name          ... (VLAN777-555)
    Flow ID[1 - 8]     ... (1)               Direction          >   (Upstream
)
    Fwd Green Packets      (839)             Fwd Green bytes        (1180946)
    Fwd Yellow Packets     (47)              Fwd Yellow bytes       (64766)
    Dscrd Green Packet     (0)               Dscrd Green bytes      (0)
```

```
    Dscrd Yellow Packe    (0)              Dscrd Yellow bytes    (0)
    Dscrd Red Packets     (0)              Dscrd Red bytes       (0)

 1. CoS ID[0 - 7]     ... (3)
>
f-Forward; b-Backward; c-Clear Statistics
ESC-prev.menu; !-main menu; &-exit                                1 M/ 1 C
```

Figure 5-36. CoS Statistics - CIR = 1 Mbps, EIR = 2 Mbps

Since the movie transmits at around 1.5Mbps and CIR = 1 Mbps and EIR = 2 Mbps using a 22 Mbps uplink, all yellow packets are forwarded as well.

4. Reduce EIR to 200 Kbps and maintain CIR at 1000 Kbps.

   Green and yellow packets are forwarded and the red packets are dropped.

```
                                    LA-210
*Monitoring>Application>Flows>CoS

    Flow Name          ... (VLAN777-555)
    Flow ID[1 - 8]     ... (1)              Direction         >   (Upstream
)
    Fwd Green Packets      (697)            Fwd Green bytes       (985270)
    Fwd Yellow Packets     (118)            Fwd Yellow bytes      (165360)
    Dscrd Green Packet     (0)              Dscrd Green bytes     (0)
    Dscrd Yellow Packe     (0)              Dscrd Yellow bytes    (0)
    Dscrd Red Packets      (247)            Dscrd Red bytes       (340366)

 1. CoS ID[0 - 7]     ... (3)
>
f-Forward; b-Backward; c-Clear Statistics
ESC-prev.menu; !-main menu; &-exit                                1 M/ 1 C
```

Figure 5-37. CoS Statistics - CIR = 1 Mbps, EIR = 200 Kbps

Since the movie transmits at around 1.5 Mbps using CIR=1 Mbps and EIR=200 Kbps, 300 Kbps worth of bandwidth is lacking and therefore the equivalent amount of red packets is dropped.

➤ **To test the bandwidth profiles for the SHDSL interface at various rates:**

1. For **BW_For_Service_777**, set the CIR to 5000 Kbps and the EIR to 3000 Kbps.

```
                                    LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                ... (2)
 2. Name                     ... (BW_for_service_777)
 3. CIR(Kbps)[0 - 100000]    ... (5000)
 4. CBS(Bytes)[0 - 32000]    ... (12176)
 5. EIR(Kbps)[0 - 100000]    ... (3000)
 6. EBS(Bytes)[0 - 32000]    ... (12176)
>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-38. Bandwidth Profile - CIR = 5 Mbps, EIR = 3 Mbps

2. For the SHDSL connection, navigate to the PCS menu (Configuration›Physical Layer›SHDSL›PCS) and set the Egress Rate Limit to 960 Kbps (*Figure 5-39*).

```
                                    LA-210
Configuration>Physical Layer>SHDSL>PCS

    PCS                                          (1)
 1. Administrative Status                        (Up)
 2. OAM (EFM)                                    (Disable)
 3. Egress Rate Limit(Kbps)[64 - 100000]      ... (960)
 4. VLAN Tag Ether Type (hex)[0 - ffff]       ... (8100)

>
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-39. Modifying the Egress Rate Limit for SHDSL

3. Navigate back to Monitoring›Application›Flows›CoS.

   Some green packets are dropped.

```
                                    LA-210
*Monitoring>Application>Flows>CoS

    Flow Name          ... (VLAN777-555)
    Flow ID[1 - 8]     ... (1)              Direction          >   (Upstream
)
    Fwd Green Packets      (2744)           Fwd Green bytes        (3787644)
    Fwd Yellow Packets     (0)              Fwd Yellow bytes       (0)
    Dscrd Green Packet     (596)            Dscrd Green bytes      (821288)
    Dscrd Yellow Packe     (0)              Dscrd Yellow bytes     (0)
    Dscrd Red Packets      (0)              Dscrd Red bytes        (0)
```

```
 1. CoS ID[0 - 7]      ... (3)
>
f-Forward; b-Backward; c-Clear Statistics
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-40. CoS Statistics - CIR = 5 Mbps, EIR = 3 Mbps, Egress Rate Limit = 1 Mbps

Since the movie transmits at around 1.5 Mbps, CIR = 5 Mbps, EIR = 3 Mbps and the SHDSL port has been limited to 1 Mbps, some green packets were dropped (*Figure 5-40*).

4. Set the CIR to 500 Kbps and the EIR to 3000 Kbps (*Figure 5-41*).
5. For the SHDSL connection, navigate to the PCS menu (Configuration›Physical Layer›SHDSL›PCS) and set the Egress Rate Limit to 1000 Kbps.

```
                                    LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                ... (2)
 2. Name                     ... (BW_for_service_777)
 3. CIR(Kbps)[0 - 100000]    ... (500)
 4. CBS(Bytes)[0 - 32000]    ... (12176)
 5. EIR(Kbps)[0 - 100000]    ... (3000)
 6. EBS(Bytes)[0 - 32000]    ... (12176)
>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-41. Bandwidth Profile - CIR = 0.5 Mbps, EIR = 3 Mbps

Since content is being transmitted at around 1.5 Mbps, CIR = 0.5 Mbps, EIR = 3 Mbps and the SHDSL port has been limited to 1 Mbps, all green packets (CIR) are forwarded and some yellow packets (EIR) are dropped (*Figure 5-42*).

```
                                    LA-210
*Monitoring>Application>Flows>CoS

    Flow Name          ... (VLAN777-555)
    Flow ID[1 - 8]     ... (1)              Direction          >   (Upstream
)
    Fwd Green Packets      (490)            Fwd Green bytes        (686244)
    Fwd Yellow Packets     (448)            Fwd Yellow bytes       (622856)
    Dscrd Green Packets    (0)              Dscrd Green bytes      (0)
    Dscrd Yellow Packets   (337)            Dscrd Yellow bytes     (475410)
    Dscrd Red Packets      (0)              Dscrd Red bytes        (0)

 1. CoS ID[0 - 7]      ... (3)
>
f-Forward; b-Backward; c-Clear Statistics
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-42. CoS Statistics - CIR = 0.5 Mbps, EIR = 3 Mbps, Egress Rate Limit = 1 Mbps

1. Set the CIR to 300 Kbps and the EIR to 200 Kbps (*Figure 5-43*).
2. For the SHDSL connection, navigate to the PCS menu (Configuration›Physical Layer›SHDSL›PCS) and set the Egress Rate Limit to 1000 Kbps.

All green and yellow packets are forwarded. The red ones are dropped.

```
                                    LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                ... (2)
 2. Name                     ... (BW_for_service_777)
 3. CIR(Kbps)[0 - 100000]    ... (500)
 4. CBS(Bytes)[0 - 32000]    ... (12176)
 5. EIR(Kbps)[0 - 100000]    ... (200)
 6. EBS(Bytes)[0 - 32000]    ... (12176)

>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-43. Bandwidth Profile - CIR = 0.5 Mbps, EIR = 0.2 Mbps

Since the movie transmits at around 1.5 Mbps, CIR = 0.5 Mbps, EIR = 0.2 Mbps and the SHDSL port has been limited to 1 Mbps, all green (CIR) and yellow (EIR) packets are forwarded and red packets are dropped (*Figure 5-44*).

```
                                    LA-210
*Monitoring>Application>Flows>CoS

    Flow Name          ... (VLAN777-555)
    Flow ID[1 - 8]     ... (1)              Direction          >   (Upstream)
    Fwd Green Packets      (664)            Fwd Green bytes        (926016)
    Fwd Yellow Packets     (170)            Fwd Yellow bytes       (234260)
    Dscrd Green Packet     (0)              Dscrd Green bytes      (0)
    Dscrd Yellow Packe     (0)              Dscrd Yellow bytes     (0)
    Dscrd Red Packets      (116)            Dscrd Red bytes        (159848)

 1. CoS ID[0 - 7]      ... (3)
>
f-Forward; b-Backward; c-Clear Statistics
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

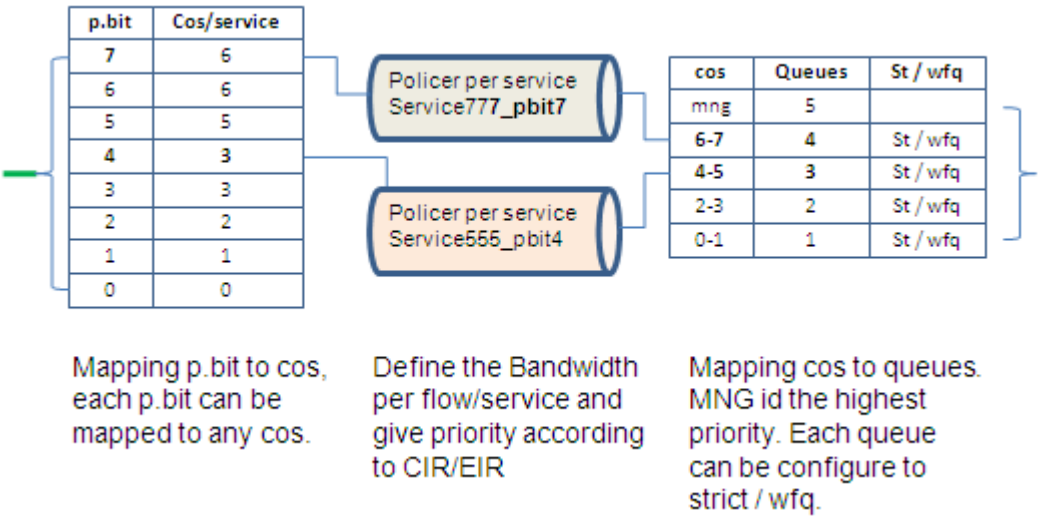
Figure 5-44. CoS Statistics - CIR = 0.5 Mbps, EIR = 0.2 Mbps, Egress Rate Limit = 1 Mbps

Priority Testing

This section explains how to test priority settings for two services with two different priority bits that you configured previously, with modified priority and with all frames transmitted at the same priority.

Using the Previously Configured Priority

This section explains how to test the priority that has been defined earlier for Service777 and Service555.


p.bit
Cos/service
7 6
6 6
5 5
4 3
3 3
2 2
1 1
0 0
Policer per service Service777_pbit7
Policer per service Service555_pbit4
cos
Queues
St / wfq
mng 5
6-7 4 St / wfq
4-5 3 St / wfq
2-3 2 St / wfq
0-1 1 St / wfq
Mapping p.bit to cos, each p.bit can be mapped to any cos.
Define the Bandwidth per flow/service and give priority according to CIR/EIR
Mapping cos to queues. MNG id the highest priority. Each queue can be configure to strict / wfq.

p.bit 7 is mapped to CoS 6 and p.bit 4 is mapped to CoS 3. CoS 3 is mapped to queue 2 and CoS 6 is mapped to queue 4. This means that frames arriving to queue 4 get higher priority than the frames arriving to queue 2.

➤ **To perform bandwidth tests on services mapped to priority bits:**

1. Configure **Service777_pbit_4** to CIR = 5000 Kbps and EIR = 2000 Kbps.

```
                                    LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                  ... (2)
 2. Name                       ... (BW_for_service_777)
 3. CIR(Kbps)[0 - 100000]      ... (5000)
 4. CBS(Bytes)[0 - 32000]      ... (12176)
 5. EIR(Kbps)[0 - 100000]      ... (2000)
 6. EBS(Bytes)[0 - 32000]      ... (12176)

>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-45. Bandwidth Profile for Service777 - CIR = 5 Mbps, EIR = 2 Mbps

2. Configure **Service555_pbit_7** to CIR = 1000 Kbps and EIR = 2000 Kbps.

```
                                    LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                ... (3)
 2. Name                     ... (BW_for_service_555)
 3. CIR(Kbps)[0 - 100000]    ... (1000)
 4. CBS(Bytes)[0 - 32000]    ... (12176)
 5. EIR(Kbps)[0 - 100000]    ... (2000)
 6. EBS(Bytes)[0 - 32000]    ... (12176)
>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-46. Bandwidth Profile for Service555 - CIR = 1 Mbps, EIR = 2 Mbps

3. For the SHDSL connection, navigate to the PCS menu (Configuration›Physical Layer›SHDSL›PCS) and set the Egress Rate Limit to 1000 Kbps (*Figure 5-39*).

   LA-210 is forwarding all green packets of **Service555_pbit_7** (*Figure 5-47*) and some of the green packets of **Service777_pbit_4** (*Figure 5-48*). The remainder is dropped.

4. To view the CoS statistics, navigate to the CoS menu (Monitoring›Application›Flows›CoS) and then press ‹**F**› to navigate to the associated CoS ID.

```
                                    LA-210
Monitoring>Application>Flows>CoS

    Flow Name          ... (VLAN777-555)
    Flow ID[1 - 8]     ... (1)              Direction          >   (Upstream)
    Fwd Green Packets      (87)             Fwd Green bytes        (5916)
    Fwd Yellow Packets     (0)              Fwd Yellow bytes       (0)
    Dscrd Green Packet     (0)              Dscrd Green bytes      (0)
    Dscrd Yellow Packe     (0)              Dscrd Yellow bytes     (0)
    Dscrd Red Packets      (0)              Dscrd Red bytes        (0)

 1. CoS ID[0 - 7]       ... (6)

>
f-Forward; b-Backward; c-Clear Statistics
ESC-prev.menu; !-main menu; &-exit                              1 M/ 1 C
```

Figure 5-47. CoS Statistics - Service555_p.bit_7 (CoS ID 6)

```
                                    LA-210
*Monitoring>Application>Flows>CoS

    Flow Name          ... (VLAN777-555)
    Flow ID[1 - 8]     ... (1)               Direction          >   (Upstream)
    Fwd Green Packets      (4729)            Fwd Green bytes        (6530429)
    Fwd Yellow Packets     (0)               Fwd Yellow bytes       (0)
    Dscrd Green Packet     (238)             Dscrd Green bytes      (327964)
    Dscrd Yellow Packe     (0)               Dscrd Yellow bytes     (0)
    Dscrd Red Packets      (0)               Dscrd Red bytes        (0)

 1. CoS ID[0 - 7]      ... (3)
>

f-Forward; b-Backward; c-Clear Statistics
ESC-prev.menu; !-main menu; &-exit                                   1 M/ 1 C
```

Figure 5-48. CoS Statistics – Service777_p.bit_4 (CoS ID 3)

The CoS statistics indicate the following:

- **Service555_pbit_7 (CoS 6):**
  All green packets are transferred since they are associated with CoS 6, which are transmitted at a higher priority than the ones associated with CoS 3.
- **Service777_pbit_4 (CoS 3):**
  Some green packets are transferred and others are dropped since the Egress rate limit (SHDSL) is set to 1 Mbps and **Service555** has a higher priority, causing its packets to be transferred first.

➤ **To modify the CIR and EIR:**

1. Configure **Service777_pbit_4** to CIR = 5000 Kbps EIR = 2000 Kbps.

```
                                    LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                ... (2)
 2. Name                     ... (BW_for_service_777)
 3. CIR(Kbps)[0 - 100000]    ... (5000)
 4. CBS(Bytes)[0 - 32000]    ... (12176)
 5. EIR(Kbps)[0 - 100000]    ... (2000)
 6. EBS(Bytes)[0 - 32000]    ... (12176)

>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                                   1 M/ 1 C
```

Figure 5-49. Bandwidth Profile for Service777 - CIR = 5 Mbps, EIR = 2 Mbps

2. Configure **Service555_pbit_7** to CIR = 0 Kbps and EIR = 2000 Kbps.

```
                                    LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                ... (3)
 2. Name                     ... (BW_for_service_555)
 3. CIR(Kbps)[0 - 100000]    ... (32)
 4. CBS(Bytes)[0 - 32000]    ... (12176)
 5. EIR(Kbps)[0 - 100000]    ... (2000)
 6. EBS(Bytes)[0 - 32000]    ... (12176)
>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-50. Bandwidth Profile for Service555 - CIR = 0 Mbps, EIR = 2 Mbps

3. For the SHDSL connection, navigate to the PCS menu (Configuration›Physical Layer›SHDSL›PCS) and set the Egress Rate Limit to 1000 Kbps (*Figure 5-39*)
4. To view the CoS statistics, navigate to the CoS menu (Monitoring›Application›Flows›CoS) and then press ‹**F**› to scroll to the associated CoS ID.

```
                                    LA-210
*Monitoring>Application>Flows>CoS

    Flow Name          ... (VLAN777-555)
    Flow ID[1 - 8]     ... (1)              Direction          >   (Upstream)
    Fwd Green Packets      (0)              Fwd Green bytes        (0)
    Fwd Yellow Packets     (258)            Fwd Yellow bytes       (17544)
    Dscrd Green Packet     (0)              Dscrd Green bytes      (0)
    Dscrd Yellow Packe     (0)              Dscrd Yellow bytes     (0)
    Dscrd Red Packets      (0)              Dscrd Red bytes        (0)

 1. CoS ID[0 - 7]      ... (6)
>
f-Forward; b-Backward; c-Clear Statistics
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-51. CoS Statistics - Service555_p.bit_7 (CoS ID 6)

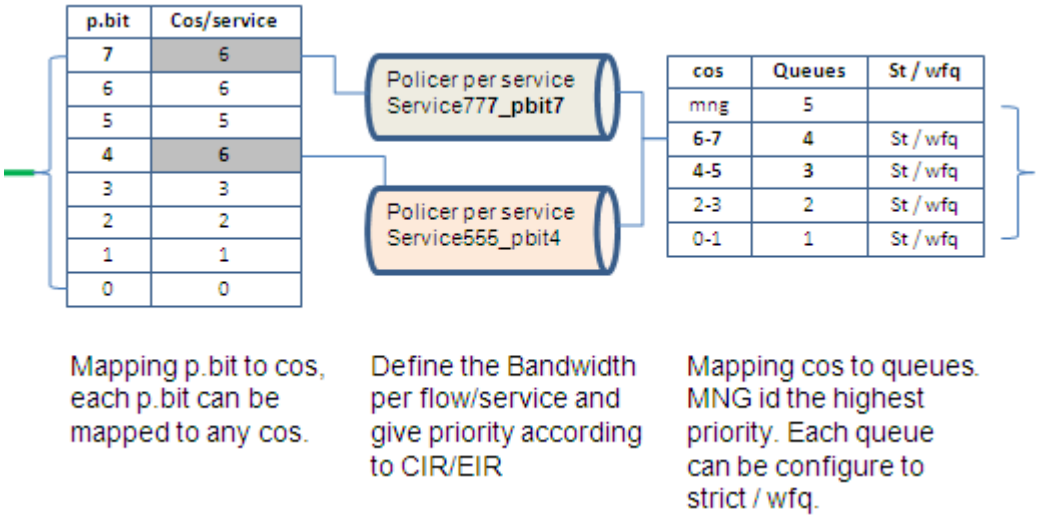
```
                                    LA-210
*Monitoring>Application>Flows>CoS

    Flow Name          ... (VLAN777-555)
    Flow ID[1 - 8]     ... (1)                Direction          >    (Upstream)
    Fwd Green Packets      (44158)            Fwd Green bytes         (60852602)
    Fwd Yellow Packets     (0)                Fwd Yellow bytes        (0)
    Dscrd Green Packet     (16430)            Dscrd Green bytes       (22635579)
    Dscrd Yellow Packe     (0)                Dscrd Yellow bytes      (31694)
    Dscrd Red Packets      (0)                Dscrd Red bytes         (0)

 1. CoS ID[0 - 7]      ... (3)
>

f-Forward; b-Backward; c-Clear Statistics
ESC-prev.menu; !-main menu; &-exit                                    1 M/ 1 C
```

Figure 5-52. CoS Statistics – Service777_p.bit_4 (CoS ID 3)

The CoS statistics indicate the following:

- **Service555_pbit_7 (CoS 6):**
  All yellow packets are transferred since they are associated with CoS 6, which are transmitted at a higher priority than the ones associated with CoS 3.
- **Service777_pbit_4 (CoS 3):**
  Some green packets are transferred and others are dropped since the Egress rate limit (SHDSL) is set to 1 Mbps and **Service555** has a higher priority, causing its packets to be transferred first.

Defining the Same Priority to All Frames



Follow the instructions under *Configuring the Units for Advanced Configurations* to map both p.bit 7 and p.bit 4 to CoS 6.

This means that frames with p.bit 4 and 7 are mapped to CoS 6 and therefore to the same queue.

➤ **To define CIR and EIR settings:**

1. Configure **Service777_pbit_4** to CIR = 10000 Kbps and EIR = 2000 Kbps.
2. Configure **Service555_pbit_7** to CIR = 1000 Kbps and EIR = 2000 Kbps.

```
                                    LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                  ... (2)
 2. Name                       ... (BW_for_service_777)
 3. CIR(Kbps)[0 - 100000]      ... (10000)
 4. CBS(Bytes)[0 - 32000]      ... (12176)
 5. EIR(Kbps)[0 - 100000]      ... (2000)
 6. EBS(Bytes)[0 - 32000]      ... (12176)

>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-53. Bandwidth Profile for Service777 - CIR = 10 Mbps, EIR = 2 Mbps

```
                                    LA-210
Configuration>Applications>QoS>Bandwidth Profiles

 1. ID[1 - 8]                  ... (3)
 2. Name                       ... (BW_for_service_555)
 3. CIR(Kbps)[0 - 100000]      ... (1000)
 4. CBS(Bytes)[0 - 32000]      ... (12176)
 5. EIR(Kbps)[0 - 100000]      ... (2000)
 6. EBS(Bytes)[0 - 32000]      ... (12176)

>
a-Add; f-Forward; b-Backward; d-Delete
ESC-prev.menu; !-main menu; &-exit                                  1 M/ 1 C
```

Figure 5-54. Bandwidth Profile for Service555 - CIR = 1 Mbps, EIR = 2 Mbps

3. For the SHDSL connection, navigate to the PCS menu (Configuration›Physical Layer›SHDSL›PCS) and set the Egress Rate Limit to 1000 Kbps (*Figure 5-39*).

   LA-210 forwards some green packets of both **Service555_pbit_7** and **Service777_pbit_4** and drops the remainder.

➤ **To test the new mappings:**

1. Start the VLC server to transmit the movie and the client to view the result.
2. Using a serial connection, connect the server PC to ETX-202 Server and log on to it.
3. Navigate to the Ping menu (*Figure 5-32*), enter the IP address of ETX-202 Client and start pinging EX-202 Client.
4. Following the instructions above, ping ETX-202 Server from ETX-202 Client.

5. If necessary, log on again to LA-210 to view the Flow statistics (Monitoring›Application›Flows) and then press ‹**F**› to scroll to the associated Flow ID.

```
                                    LA-210
*Monitoring>Application>Flows>CoS

    Flow Name          ... (VLAN777-555)
    Flow ID[1 - 8]     ... (1)               Direction          >   (Upstream)
    Fwd Green Packets      (8285)            Fwd Green bytes        (1114948)
    Fwd Yellow Packets     (0)               Fwd Yellow bytes       (0)
    Dscrd Green Packets    (681)             Dscrd Green bytes      (92140)
    Dscrd Yellow Packets   (0)               Dscrd Yellow bytes     (0)
    Dscrd Red Packets      (0)               Dscrd Red bytes        (0)

 1. CoS ID[0 - 7]      ... (6)
f-Forward; b-Backward; c-Clear Statistics
ESC-prev.menu; !-main menu; &-exit                                    1 M/ 1 C
```

Figure 5-55. Flow Statistics – Service777_p.bit_4 (CoS ID 6)

```
                                    LA-210
Diagnostic>Application>Flows>CoS

    Flow Name          ... (VLAN777-555)
    Flow ID[1 - 8]     ... (1)               Direction          >   (Upstream)
    Fwd Green Packets      (8285)            Fwd Green bytes        (1114948)
    Fwd Yellow Packets     (0)               Fwd Yellow bytes       (0)
    Dscrd Green Packets    (681)             Dscrd Green bytes      (92140)
    Dscrd Yellow Packets   (0)               Dscrd Yellow bytes     (0)
    Dscrd Red Packets      (0)               Dscrd Red bytes        (0)

 1. CoS ID[0 - 7]      ... (3)
f-Forward; b-Backward; c-Clear Statistics
ESC-prev.menu; !-main menu; &-exit                                    1 M/ 1 C
```

Figure 5-56. Flow Statistics – Service777_p.bit_4 (CoS ID 3)

Both services, **Service555_pbit_7** and **Service777_pbit_4** are associated with the same CoS, therefore the results are identical.

```
                                    LA-210
Diagnostics>Ping

1. Destination IP Address               ... (0.0.0.0)
2. Number of Frames to Send[0 - 50]     ... (1)
3. Send Ping
4. Stop Ping

>
Please select item <1 to 4>

ESC-prev.menu; !-main menu; &-exit                                    1 Mngr/s
------------------------------------------------------------------------------
Reply  from  host  172.17.182.24  time = 310m
Reply  from  host  172.17.182.24  time = 320m
Reply  from  host  172.17.182.24  time = 320m
Reply  from  host  172.17.182.24  time = 320m
Reply  from  host  172.17.182.24  time = 320m
Host 172.17.182.24 request timed out.
Reply  from  host  172.17.182.24  time = 320m
```

Figure 5-57. Ping Results - ETX-202 Server to ETX-202 Client

The ping test shows that not all the pings are replied to and the ones that are replied to are replied to with a delay of 300 msec. The reason is that all frames are mapped to the same queue and the SHDSL port is limited to 1 Mbps and the green packets are larger than 1 Mbps.

Chapter 6

Diagnostics and Troubleshooting

This section describes how to:

- Monitor the system performance
- Display status and statistics
- Display system messages
- Detect errors
- Troubleshoot the device
- Perform connectivity tests.

6.1 Monitoring Performance

The software provides access to the following status information:

- System level – MAC address, connection status, and Event Log file
- Physical level – Ethernet and SHDSL port status
- Application level – MAC table.

The status information is available via the Monitoring menu.

Displaying System Status Informathion

The System menu shows the interface connection status and Event Log file. For a description of system messages, which are displayed via the Event Log file, refer to *Displaying the Event Log File*.

➤ **To display interface connection information:**

1. Select Main Menu›**Monitoring**.

   The Monitoring screen appears (see *Figure 6-1*).

2. Select **System**.

   The Monitoring System screen appears (see *Figure 6-2*).

3. Select **Interface Status**.

   The Interface Status screen appears (see *Figure 6-3*). The parameters are described in *Table 6-1*.

```
                                    LA-210
Main Menu > Monitoring

1. System                    >
2. Physical Ports            >
3. Application               >

C-Clear All Statistics
ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 6-1. Monitoring Screen

```
                                    LA-210
Main Menu > Monitoring > System

MAC address                  … (00-D2-20-10-20-30)
System Up Time                  (44:20:12)
Date                            (0000-00-00)
Time                            (0:06:57)
Security Key                    (SSL+SSH)

1. Interface Status             []
2. Event log                    []
3. Radius Statistics            []
4. Connected Managers           []

>
ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 6-2. Monitoring System Screen

```
                                    LA-210
Main Menu > Monitoring > System > Interface Status
 Description        Type               Activation        Operation   Speed
 ETH Port 1         Fast Eth           Up                Down        0
 ETH Port 2         Fast Eth           Up                Down        0
 ETH Port 3         Fast Eth           Up                Down        0
 ETH Port 4         Fast Eth           Up                Down        0
 SDHSL Port 1       Multirate HDSL2    Up                Up          0
 Logical Port       Fast Eth           Up                Down        0
 Bridge Port 1      Bridge Port        Up                Up          0

ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 6-3. Interface Status Screen

Table 6-1. Interface Status Parameters

Parameter	Description
Interface Description	Fast Ethernet and SHDSL port
Type	The type of the interface
Activation	Whether the interface is enabled (Up) or disabled (Down), as user defined via the Ethernet and SHDSL menus (see *Chapter 4*).
Operation	Actual operational status of the link (Up or Down).

Displaying the Physical Port Status

You can view the status of the unit's physical ports.

For a description of the Ethernet and SHDSL port statistics, refer to *Displaying Statistics*.

Displaying the Ethernet Port Status

➤ **To display the Ethernet port status:**

1. From the Ethernet menu (Monitoring › Physical Ports › Ethernet), select **Status**.

   The Fast Ethernet Status screen appears (see *Figure 6-4*). The parameters are described in *Table 6-2*.

2. Press ‹**F**› to select the port number.

```
                                LA-210
Main Menu > Monitoring > Physical Ports > Ethernet > Status

Port                            (1)

Administrative Status           (Enable)
Operation Status                (Up)
Speed & Duplex                  (100Mbps - Full Duplex)
Flow Control                    (Enable)

F - Forward; B - Backward
ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 6-4. Ethernet Status Screen

Table 6-2. Ethernet Status Parameters

Parameter	Description
Port	The port slot number to be handled.
Admistrative Status	Whether the interface is enabled or disabled.
Operation Status	The actual operational status of the link (Up or Down).

Parameter	Description
Speed & Duplex	The current data rate and duplex mode of the link (100 – full, 100 –half, 10 – full, or 10 - half).
Flow Control	Whether flow control is enabled or disabled.

Displaying the SHDSL Line Status

➤ To display the SHDSL Line status:

1. From the SHDSL menu (Monitoring › Physical Ports › Line), select **Status**.

   The SHDSL Status screen appears (see *Figure 6-7*).

```
                              LA-210
Main Menu > Monitoring > Physical Ports > SHDSL > Status

1. Line                                 >
2. PCS (if TC Layer = 64-65-octet)      >

>

ESC-Previous menu; !-Main Menu; &-Exit
```

Figure 6-5. SHDSL Screen

2. From the SHDSL menu (Monitoring › Physical Ports › SHDSL › Status), select **Line**.

   The SHDSL Line Status screen appears (see *Figure 6-7*).

3. To view an additional SHDSL line, press ‹**F**› or ‹**B**› to scroll forward or backward through the list respectively.

```
                              LA-210
Main Menu > Monitoring > Physical Ports > SHDSL > Status > Line

Line                            (1)

Administrative Status           (Up)
Operation Status                (Up)
SHDSL Mode                      (STU-R)
PSD Mask                        (Symmetric)
SHDSL Transmission Mode         (Annex B/G)
Wiring                          (2 Wire)
Line State                      (PreActivation)
Line Rate                       (0)
Current Noise Margin            (0)
Current Loop Attenuation        (0)

f-Forward; b-Backward
ESC-Previous menu; !-Main Menu; &-Exit
```

Figure 6-6. SHDSL Line Status Screen

Table 6-3. SHDSL Line Status Parameters

Parameter	Description
PCS (Physical Coding Sublayer)	The SHDSL PCS number to be handled.
Admistrative Status	Indicates whether the interface is up or down.
Operation Status	The actual operational status of the SHDSL PCS (Up or Down).
SHDSL Mode	The SHDSL mode (STU-C or STU-R).
PSD Mask	PSD (power spectral density) mask for the SHDSL line (symmetric or asymmetric)
SHDSL Transmission Mode	Contains the current Power Spectral Density (PSD) regional setting of the SHDSL span (Annex A or Annex B)
Wiring	Indicates the SHDSL port wiring (2 Wire, 4 Wire or 8 Wire)
Line State	The current operational state (PreActivation, activation or data transfer)
Line Rate	The actual line rate (64 – 5696 kbps)
Curent Noise Marging	The current SNR margin for this endpoint (0 – 15db)
Current Loop Attenuation	The current loop attenuation for this endpoint (0 – 127db)

Displaying the SHDSL PCS Port Status

➤ **To display the SHDSL PCS port status:**

1. From the SHDSL menu (Monitoring > Physical Ports > SHDSL), select **Status**.

   The SHDSL Status screen appears (see *Figure 6-7*).

2. From the SHDSL menu (Monitoring > Physical Ports > SHDSL >Status), select **PCS**.

   The SHDSL PCS Status screen appears (see *Figure 6-7*). The parameters are described in *Table 6-4*.

```
                              LA-210
Main Menu > Monitoring > Physical Ports > SHDSL > Status > PCS

PCS (Physical Coding Sublayer) (1)

Administrative Status          (Up)
Operation Status               (Up)

ESC-Previous menu; !-Main Menu; &-Exit
```

Figure 6-7. SHDSL PCS Status Screen

Table 6-4. SHDSL PCS Status Parameters

Parameter	Description
PCS (Physical Coding Sublayer)	The SHDSL PCS number to be handled.
Admistrative Status	Indicates whether the interface is up or down.
Operation Status	The actual operational status of the SHDSL PCS (Up or Down).

Displaying Application-Level Status

At the application level, the unit provides information on the MAC addresses (static and learned) and their bridge port assignments, as well as VLAN IDs and their bridge port assignments.

➤ To display the MAC table:

- From the Bridge menu (Monitoring › Application › Bridge), select **View MAC Table**.

  The MAC Table screen appears (*Figure 6-8* and *Figure 6-9*). The parameters are described in *Table 6-5*.

```
                              LA-210
Main Menu > Monitoring > Application > Bridge > View MAC Table

      VLAN ID   MAC address          Bridge port        Status

  1      1      11-11-11-11-11-11        1             Static
| 2      1      22-22-22-22-22-22        2             Dynamic
v 3      2      33-33-33-33-33-33        3             Static
  4      3      44-44-44-44-44-44        3             Dynamic
  5      4      55-55-55-55-55-55        5             Dynamic

ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 6-8. View MAC Table (VLAN-Aware)

```
                              LA-210
Main Menu > Monitoring > Application > Bridge > View MAC Table

      MAC address           Bridge port             Status

  1   11-11-11-11-11-11          1                  Static
| 2   22-22-22-22-22-22          2                  Dynamic
V 3   33-33-33-33-33-33          3                  Static
  4   44-44-44-44-44-44          3                  Dynamic
  5   55-55-55-55-55-55          5                  Dynamic

ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 6-9. View MAC Table (VLAN-Unaware)

Table 6-5. View MAC Table Parameters

Parameter	Description
VLAN ID (VLAN aware mode only)	The VLAN ID corresponding to the MAC address (1 – 4094).
MAC Address	The destination MAC address in a frame to which this entry's filtering information applies.
Bridge Port	The port number of the port from which a frame must be received in order for this entry's filtering information to apply.
Status	The status of the entry (Static or Dynamic).

➤ **To display the OAM status:**

- From the End-to-End menu (Monitoring › Application › OAM › End-to-End), select **Status**.

The OAM Status screen appears as illustrated in *Figure 6-10*).

```
                              LA-210
Main Menu > Monitoring > Application > OAM > End-to-End >
Status

   Flow ID                        ... (Put your string here)
   Flow SP VLAN[1 - 4094]         ... (5)
   Remote Mep Address             ... (00-00-00-00-00-00)
   Flow Status                   >   (Not Applicable)

1. Flow [1 - 8]                  ... (1)
2. Remote Mep ID[1 - 8191]       ... (1)

ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 6-10. OAM Status Screen

Table 6-6. OAM Status

Parameter	Description
Flow ID	The Ethernet virtual connection's ID.
Flow SP VLAN[1 – 4094]	The destination MAC address in a frame to which this entry's filtering information applies.
Remote Mep Address	Maintenance entity group's address
Flow ID[1 – 8]	Ethernet virtual connection
Remote Mep ID[1 – 8191]	Reemote ID of the Maintenance entity group

6.2 Displaying Statistics

You can display statistical data for the Ethernet and SHDSL ports as well as End-to-End statistics for the OAM.

Displaying Ethernet Port Statistics

You can display statistical data for the Ethernet ports.

➤ **To view Ethernet statistics:**

1. From the Ethernet menu (Monitoring › Physical Ports › Ethernet), select **Statistics**.

   The Fast Ethernet Statistics screen appears (see *Figure 6-11*). The parameters are described in *Table 6-7*.

2. Press ‹**F**› to select the port number.

```
                              LA-210
Main Menu > Monitoring > Physical Ports> Ethernet > Statistics

    Port                            (1)
    Rx Correct Frames               (166185)
    Rx Correct Octets               10635840)
    Rx Alignment Error              (0)
    Rx FCS Errors                   (0)
    Rx Congestion Dropped Frames    (0)
    Tx Correct Frames               (13793)
    Tx Correct Octets               (882752)
    Tx Single Collision             (0)
    Tx Collision                    (0)
    Tx Multiple Collision           (0)
    Tx Deferred Transmissions       (0)
    Tx Late Collisions              (0)
    Tx Congestion Dropped Frames    (0)

F-Forward; B-Backward; C-Clear statistics
ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 6-11. Fast Ethernet Statistics Screen

Table 6-7. Fast Ethernet Statistics Parameters

Parameter	Description
Port	The selected port slot number.
Rx Correct Frames	The number of correct frames received.
Rx Correct Octets	The number of octets (bytes) received
Rx Alignment Error	The number of frames received with a valid length, but with invalid FCS and a non-integral number of octets.

Parameter	Description
Rx FCS Errors	The number of frames with FCS errors received by this port.
Rx Congestion Dropped Frames	The number of frames that are discarded due to a lack of buffer space.
Tx Correct Frames	The number of frames successfully transmitted.
Tx Correct Octets	The number of octets (bytes) successfully tranmsmitted.
Tx Single Collision	The number of transmission attempts that experienced a single collision.
Tx Collision	The number of transmission attempts that experienced a collision.
Tx Multiple Collision	The number of transmission attempts that experienced multiple collisions
Tx Deferred Transmissions	The number of transmission attempts deferred in order to avoid a collision.
Tx Late Collisions	The number of transmission attempts that experienced late collisions.
Tx Congestion Dropped Frames	The number of frames discarded due to a lack of buffer space.

Clearing Ethernet Port Statistics

➤ **To clear all Ethernet and SHDSL statistics:**

- In the Monitoring menu (*Figure 6-1*), press ‹C› to clear all Ethernet and SHDSL statistics.

➤ **To clear all Ethernet statistics:**

- In the Ethernet screen, press ‹C› to clear all Ethernet statistics.

➤ **To clear port statistics:**

- In the Ethernet Statistics screen (*Figure 6-11*), press ‹C› to clear the selected Ethernet port statistics.

Displaying SHDSL Port Statistics

You can display statistical data for the SHDSL ports.

Displaying SHDSL PCS Port Statistics

➤ To view SHDSL PCS port statistics:

1. From the PCS menu (Monitoring › Physical Ports › SHDSL › Statistics › PCS), select **Statistics**.

   The SHDSL PCS Statistics screen appears as illustrated in *Figure 6-12*. The statistics are described in *Table 6-8*.

2. Press ‹**F**› to select the PCS number.

```
                                LA-210
Main Menu > Monitoring > Physical Ports > SHDSL > Statistics >
PCS

PCS Number                (1)

RX Total Errors           (0)
RX Total Frames           (0)
RX Total Bytes            (0)
TX Total Frames           (0)
TX Total Bytes            (0)
TX Dropped Frames         (0)

F-Forward; B-backward; C - Clear PCS Statistics
ESC-Previous menu; !-Main Menu; &-Exit
```

Figure 6-12. SHDSL PCS Statistics Screen

Table 6-8. SHDSL PCS Statistics Parameters

Parameter	Description
PCS Number	The selected SHDSL PCS number.
TX Total Frames	The total number of frames transmitted.
RX Total Frames	The total number of frames received.
RX Total Errors	The total number of errors received.

Displaying SHDSL Line Statistics

➤ To view SHDSL line statistics:

- From the Line menu (Monitoring › Physical Ports › SHDSL › Statistics › Line), select **Statistics**.

```
                                LA-210
Main Menu > Monitoring > Physical Ports > SHDSL > Statistics >
Line

Line                                (1)

1. Current Interval
2. 15 Min. Intervals
3. Current Day Interval
4. Day Intervals
5. Accumulated Data

F-Forward; B-backward; C-Clear statistics
ESC-Previous menu; !-Main Menu; &-Exit
```

Figure 6-13. SHDSL Line Statistics Screen

Table 6-9. SHDSL Line Statistics Parameters

Parameter	Description
Line	The line number for which the statistics are displayed
Current Interval	The statistics counters in current 15 minutes intervals.
15 Min. Intervals	The statistics counters in intervals of 15 minutes. (Interval number 0 represents the current counters.)
Current Day Interval	The statistics counters in current 1 day intervals.
Day Intervals	The statistics counters in intervals of 1 day. (Interval number 0 represents the current counters.)
Accumulated Data	Accumulated statistics counters.

Displaying SHDSL Line Current Interval Statistics

➤ To view SHDSL Line Current Interval statistics:

1. From the Line Statistics (Monitoring›Physical Ports›SHDSL› Statistics›Line), select Current Interval.

   The SHDSL Line Current Interval Statistics screen appears
   Displaying SHDSL Line 15 Minute Intervals Statistics

➤ To view SHDSL Line 15 minute intervals statistics:

1. From the Line Statistics menu (Monitoring›Physical Ports›SHDSL›Statistics›Line), select **15 Min. Intervals**.

   The SHDSL Line 15 Minute Intervals Statistics screen appears (see *Figure 6-14*). The statistics are described in *Table 6-10*.

2. Press ‹**F**› to select the Line number.
3. Press ‹**F**› to select the Interval number.

```
                                LA-210
Main Menu > Monitoring > Physical Ports > SHDSL > Statistics >
Line > 15 Min Intervals

Line                                          (1)
Interval Number [1-96]                        (1)

ES                              (0)
UAS                             (0)
SES                             (0)
LOSWS                           (0)
CRC Anomalies                   (0)

F-Forward; B-Backward ; ^F-Forward(Intervals) ; ^B-
Backward(Intervals)
ESC-Previous menu; !-Main Menu; &-Exit
```

Figure 6-14. SHDSL PME 15 Minute Intervals Statistics Screen

Table 6-10. SHDSL PME 15 Minute Intervals Statistics

Parameter	Description
Line	The current SHDSL line.
Interval Number	The Performance Data Interval number.
ES	The number of Errored Seconds (ES) during the interval.
UAS	The number of unavailable Seconds (UAS) during the interval.
SES	The number of Severely Errored Seconds (ES) during the interval.
LOSWS	The number of Loss of Sync Word (LOSW) Seconds during the interval.
CRC Anomalies	The number of CRC anomalies during the interval.

Displaying SHDSL Line Current DayInterval Statistics

➤ To view SHDSL Line Current Interval statistics:

1. From the Line Statistics (Monitoring›Physical Ports›SHDSL›Statistics›Line), select Current Day Interval.

   The SHDSL Line Current Day Interval Statistics screen appears (see *Figure 6-15*). The statistics are described in *Table 6-11*.

2. Press ‹F› to select the Line number.

```
                                LA-210
Main Menu > Monitoring > Physical Ports > SHDSL > Statistics >
Line > Current Day Interval

Line                                              (1)

ES                              (0)
UAS                             (0)
SES                             (0)
LOSWS                           (0)
CRC Anomalies                   (0)
Elapsed Time                    (900)

F-Forwards ; B-Backwards
ESC-Previous menu; !-Main Menu; &-Exit
```

Figure 6-15. SHDSL Line Current Day Interval Statistics Screen

Table 6-11. SHDSL Line Current Day Interval Statistics

Parameter	Description
Line	The selected SHDSL Line number.
ES	The number of Errored Seconds (ES) during the current day.
UAS	The number of unavailable Seconds (UAS) during the current day.
SES	The number of Severely Errored Seconds (ES) during the current day.
LOSWS	The number of Loss of Sync Word (LOSW) Seconds during the current day.
CRC Anomalies	The number of CRC anomalies during the current day.
Elapsed Time	The number of seconds that have elapsed since the beginning of the current 1-day interval.

Displaying SHDSL Line Day Intervals Statistics

➤ To view SHDSL Line Day Intervals statistics:

1. From the PME Statistics (Monitoring›Physical Ports›SHDSL›Statistics›Line), select **Day Intervals**.

   The SHDSL Line Day Intervals Statistics screen appears (see *Figure 6-16*). The statistics are described in *Table 6-12*.

2. Press ‹**F**› to select the Line number.
3. Press ‹**^F**› to select the interval number.

```
                                    LA-210
Main Menu > Monitoring > Physical Ports > SHDSL > Statistics > Line > Day
Intervals

Line                                          (1)
Interval Number [1-7]

ES                          (0)
UAS                         (0)
SES                         (0)
LOSWS                       (0)
CRC Anomalies               (0)

F-Forward; B-Backward; ^F-Forward(Intervals) ; ^B-Backward(Intervals)
ESC-Previous menu; !-Main Menu; &-Exit
```

Figure 6-16. SHDSL Line Day Intervals Statistics Screen

Table 6-12. SHDSL Line Day Intervals Statistics

Parameter	Description
Line	The selected SHDSL Line number.
Interval Number	The History Data Interval number.
ES	The number of Errored Seconds (ES) during the 1-day interval.
UAS	The number of unavailable Seconds (UAS) during the 1-day interval.
SES	The number of Severely Errored Seconds (ES) during the 1-day interval.
LOSWS	The number of Loss of Sync Word (LOSW) Seconds during the 1-day interval.
CRC Anomalies	The number of CRC anomalies during the 1-day interval.

Displaying SHDSL PME Accumulated Data Statistics

➤ To view SHDSL PME Accumulated Data statistics:

1. From the PME Statistics (Monitoring›Physical Ports›SHDSL›Statistics›Line), select Accumulated Data.

   The SHDSL Line Day Intervals Statistics screen appears (see *Figure 6-17*). The statistics are described in *Table 6-13*.

2. Press <F> to select the Line number.
3. Press <^F> to select the Interval number.

```
                                LA-210
Main Menu > Monitoring > Physical Ports > SHDSL > Statistics >
Line > Accumulated Data

ES                              (0)
UAS                             (0)
SES                             (0)
LOSWS                           (0)
CRC Anomalies                   (0)
Accumulated Time                (0)

ESC-Previous menu; !-Main Menu; &-Exit
```

Figure 6-17. SHDSL Line Accumulated Data Statistics Screen

Table 6-13. SHDSL Line Accumulated Data Statistics

Parameter	Description
ES	The number of Errored Seconds (ES) on this endpoint since it was last restarted.
UAS	The number of Unavailable Seconds (UAS) on this endpoint since it was last restarted.
SES	The number of Severely Errored Seconds (SES) on this endpoint since it was last restarted.
LOSWS	The number of Loss of Sync Word (LOSW) Seconds on this endpoint since it was last restarted
CRC Anomalies	The number of CRC anomalies on this endpoint since it was last restarted.
Accumulated Time	The time (in hundredths of a second) since the accumulated counters were last re-initialized.

Clearing the SHDSL Port Statistics

➤ **To clear all Ethernet and SHDSL statistics**

- In the Monitoring screen (see *Figure 6-1*), press ‹**C**› to clear all Ethernet and SHDSL statistics.

➤ **To clear all SHDSL PCS and PME statistics:**

- In the SHDSL PCS Statistics screen (see *Figure 6-12*), select **Clear All SHDSL Statistics** to clear all SHDSL PCS and PME statistics.

➤ **To clear SHDSL PCS statistics:**

- In the SHDSL PCS Statistics screen (see *Figure 6-12*), press ‹**C**› to clear the SHDSL PCS statistics.

➤ **To clear the SHDSL PME statistics:**

- In the SHDSL PME Statistics screen (see *Figure 6-13*), press ‹**C**› to clear the SHDSL PME statistics.

Displaying Flow Statistics

You can display the number of forwarded and discarded packets while transmitting content. An example for flow statistics while transmitting a movie and changing parameters is discussed in *Chapter 5*.

➤ **To display flow statistics:**

- From the Flows menu (Monitoring›Application›Flows), choose the desired flow.

  To choose a flow, either select **Flow** ID and enter the associated flow ID or press ‹**F**› or ‹**B**› to navigate to that flow.

  The statistics of the desired flow are displayed as illustrated in *Figure 6-18*.

```
                                    LA-210
Monitoring>Application>Flows

    Flow Name            ... (Put your…)  Direction              >  (Upstream)
    Fwd Green Pkts           (0)          Fwd Green bytes           (0)
    Fwd Yellow Pkts          (0)          Fwd Yellow bytes          (0)
    Dscrd Green Pkts         (0)          Dscrd Green bytes         (0)
    Dscrd Yellow Pkts        (0)          Dscrd Yellow bytes        (0)
    Dscrd Red Pkts           (0)          Dscrd Red bytes           (0

 1. Flow ID[1-8]         ... (1)
 2. CoS                  >

>
F-Forward; b-Backward; ^F-Frw(Port);^B-Bkw(Port)

ESC-prev.menu; !-main menu; &-exit                                  1 Mngr/s
```

Figure 6-18. End-to-End Statistics (15-Minute Interval)

➤ **To display the CoS statistics for a specific flow:**

- From the Flows menu (Monitoring›Application›Flows), select **CoS**.

  CoS statistics for the first CoS in the list appear.

- To choose another CoS, select **CoS** ID and enter the associated ID or press ‹**F**› or ‹**B**› to navigate to that CoS.

```
                                    LA-210
Monitoring>Application>Flows
    Flow Name            ... (Put your…)  Direction              >  (Upstream)
    Fwd Green Pkts           (0)          Fwd Green bytes           (0)
    Fwd Yellow Pkts          (0)          Fwd Yellow bytes          (0)
    Dscrd Green Pkts         (0)          Dscrd Green bytes         (0)
    Dscrd Yellow Pkts        (0)          Dscrd Yellow bytes        (0)
    Dscrd Red Pkts           (0)          Dscrd Red bytes           (0

 1. Flow ID[1-8]         ... (1)
 2. CoS                  >

>
F-Forward; b-Backward; ^F-Frw(Port);^B-Bkw(Port)

ESC-prev.menu; !-main menu; &-exit                                  1 Mngr/s
```

Figure 6-19. End-to-End Statistics (15-Minute Interval)

Displaying End-to-End Statistics for OAM

You can display end-to-end connectivity and performance monitoring data for the existing flows and the associated services. The statistics are available for the 15-minute and 24-hour periods.

➤ **To display the End-to-End statistics:**

1. From the End-To-End menu (Monitoring›Application›OAM›End-To-End), select **Statistics**.

   The Statistics menu appears.

2. From the Statistics menu, select the following:
   - **15 Min Intervals**. OAM statistics for a selected 15-min interval
   - **24 Hours Counters**. OAM statistics for the last 24 hours
   - **Service Counters**. Total OAM statistics collected since the service was enabled
3. Selected OAM statistic screen in displayed (see *Figure 6-18* and *Figure 6-19*). *Table 6-14* and *Table 6-15* explain the OAM statistic parameters.
4. Type ‹**F**› or ‹**B**› to select a flow.
5. Press ‹**Ctrl** + **F**› or ‹**Ctrl** + **B**› to select an interval (1–96).

Note *No interval selection is available for the 24-hour statistics.*

```
                                    LA-210
Monitoring>Application>OAM>End-To-End>Statistics>15 Min. Intervals

    Frames Above Delay Obj.... (0)          Elapsed Time          ... (102767)
    Frames Below Delay Obj.... (0)
    Frames Above DV Obj.   ... (0)          Min. RT Delay (Msec)   ... (0.0)
    Frames Below DV Obj.   ... (0)          Avg. RT Delay (Msec)   ... (0.0)
    Frames Transmitted     ... (101902)     Max. RT Delay (Msec)   ... (0.0)
    Frames Loss            ... (0)
    Unavailable Seconds    ... (101899)     Avg. DV                ... (0.0)
                                            Max. DV                ... (0.0)
 1. MD ID                  ... (0)
 2. MA ID                  ... (1)
 3. MEP ID[1 - 8191]       ... (2)
 4. Service                ... (1)
 5. Interval               ... (0)

>
Please select item <1 to 5>

ESC-prev.menu; !-main menu; &-exit                                  1 Mngr/s
```

Figure 6-20. End-to-End Statistics (15-Minute Interval)

Table 6-14. End-to-End Statistics Parameters

Parameter	Description
Frames Above Delay Obj.	Number of frames that exceeded delay objective
Frames Below Delay Obj.	Number of frames below or equal delay objective
Frames Above DV Obj.	Number of frames that exceeded delay variation objective
Frames Below DV Obj.	Number of frames below or equal delay variation objective
Frames Transmitted	Total number of OAM frames transmitted in the current interval
Frames Lost	Number of frames lost in the current interval
Unavailable Seconds	Number of seconds during which the service was unavailable in the current interval
Elapsed Time	Time (in seconds) elapsed from beginning of the interval 0–900
Min. RT Delay	Minimum round trip delay (in mseconds) calculated in the interval (or up to elapsed time in current interval)
Avg. RT Delay	Average round trip delay (in mseconds) calculated in the interval (or up to elapsed time in current interval)
Max. RT Delay	Maximum round trip delay (in mseconds) calculated in the interval (or up to elapsed time in current interval)
Avg. DV	Average delay variation (in mseconds) calculated in the interval (or up to elapsed time in current interval)
Max. DV	Maximum delay variation (in mseconds) calculated in the interval (or up to elapsed time in current interval)

```
                                    LA-210
Monitoring>OAM>End-To-End>Statistics>Service Counters
    Flow                          ... (1)
    Service                       ... (1)


    OAM transmitted frames counter... (2087328632)
    OAM Frames lost counter       ... (0
    OAM Frame loss ratio(*E-10)   ... (0)
    Elapsed time                  ... (1487)
    Unavailable seconds           ... (0)
    Unavailability ratio(*E-10)   ... (0)
>
F - Forward(SVC); B - Backward(SVC); C-Reset Counters
ESC-prev.menu; !-main menu; &-exit                                  1 Mngr/s
```

Figure 6-21. End-to-End Service Counters

Table 6-15. End-to-End Service Counters

Parameter	Description
OAM Transmitted Frames Counter	Total number of OAM frames transmitted since the service was enabled
OAM Frames Loss Counter	Total number of OAM frames lost since the service was enabled
OAM Frame Loss Ratio	Total number of lost OAM frames divided by total number of transmitted OAM frames since the service was enabled
Elapsed Time	Time (in seconds) elapsed since the service was enabled
Unavailable Seconds	Total number of unavailable seconds since the service was enabled
Unavailability Ratio	Total number of unavailable seconds divided by elapsed time

Viewing Radius Statistics

➤ **To view Radius statistics:**

- Navigate to Main Menu › Monitoring › System › **Radius Statistics**.

The Radius Statistics screen appears as illustrated in *Figure 6-20*.

```
                              LA-210
Monitoring>System>Radius Statistics

                        Server1 Server2 Server3 Server4
 Access Requests        0       0       0       0
 Access Retransmits     0       0       0       0
 Access Accepts         0       0       0       0
 Access Rejects         0       0       0       0
 Access Challenges      0       0       0       0
 Malformed Response     0       0       0       0
 Bad Authenticators     0       0       0       0
 Pending Requests       0       0       0       0
 Timeouts               0       0       0       0
 Unknown Types          0       0       0       0
 Packets Dropped        0       0       0       0
ESC-prev.menu; !-main menu; &-exit; ?-help
```

Figure 6-22. Radius Statistics Screen

6.3 Handling Alarms and Traps

LA-210 maintains a log file, which can hold up to 1,000 system messages. All events are time-stamped.

Traps that are the result of events that were already reported by a different trap may not be repeated. For example, LOC traps will not be sent if the physical layer trap, such as LOS, was sent and the physical layer problem still exists.

The events are layered hierarchically, for example physical layer events/traps for Loop Attenuation and SNR Margin are threshold triggered, so that an event/trap is sent only if the threshold was exceeded.

Threshold can be configured for up to 8000 events per second.

The Event Log file contents can be viewed via an ASCII control terminal or a Network Management Station (NMS).

The contents can be cleared at any time.

Note *All traps (alarm and system) can be masked per manager, as described in Chapter 4.*

Displaying the Event Log File

LA-210 has an integrated NTP client. The NTP client is used as a means to receive the date and time from the network. When the NTP server is properly configured and accessible, the device displays the real date and time as was received from the NTP server, instead of the system uptime, which is the default state.

When the real date and time are not available, the log file messages are recorded with the date 00-00-0000 and system uptime. Once the NTP server becomes available, all messages (including those already received) appear with the real date and time.

➤ **To access the Event Log file:**

1. From the System menu (Monitoring > System), select **Event Log**.

   The Event Log screen appears as illustrated in *Figure 6-21* and *Figure 6-22*.
   Table 6-16 and *Table 6-17* present the event types that appear in the Event Log file.

2. Use the arrow keys to scroll the event list up and down, left and right.

```
                                    LA-210
Main Menu > Monitoring > System > Event Log

    Source       Description   Information   Severity   Date        Time
1   PME Port 1   LINK_DOWN     PME port      Major      00-00-0000  00:00:01
2   PME Port 2   LINK_UP       PME port      Major      00-00-0000  00:00:02
3   Eth Port 4   LINK_DOWN     Eth port      Major      00-00-0000  00:00:04

C - Clear Table
ESC-Previous menu; !-Main menu; &-Exit;  ?-Help
```

Figure 6-23. Typical Log File Before NTP Server is Accessible

```
                                    LA-210
Main Menu > Monitoring > System > Event Log

    Source       Description   Information   Severity   Date        Time
1   PME Port 1   LINK_DOWN     PME port      Major      04-07-1776  00:00:01
2   PME Port 2   LINK_UP       PME port      Major      02-06-1946  00:00:02
3   Eth Port 4   LINK_DOWN     Eth port      Major      01-10-1949  00:00:04

C - Clear Table
ESC-Previous menu; !-Main menu; &-Exit;  ?-Help
```

Figure 6-24. Typical Log File After NTP Server is Accessible

Table 6-16. Ethernet Event List

Parameter	Severity	Description
Link up	Major	Port is up.
Link down	Major	Port is down.
TFTP failure	Event	Failed in processing software download.
SNMP Authentication failure	Event	Wrong community.
TFTP start	Event	TFTP began.
TFTP finish	Event	TFTP ended.
Telnet Manager list restriction	Event	TELNET session from an unauthorized IP address.
WEB Manager list restriction	Event	WEB session from an unauthorized IP address.
SNMP Manager list restriction	Event	SNMP from an unauthorized IP address.

Table 6-17. Trap List

Trap	Description
Link Up	Signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state).
Link Down	Signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state).
Cold Start	Signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.
Warm Start	Signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.
Authentication Failure	Signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
TFTP Status	This trap is sent whenever the status of TFTP changed.
Status Change	This trap is sent whenever the state of the entity the agent is responsible for changed.
SNR Margin Threshold Exceeded	Indicates that the SNR margin threshold (as per the hdsl2ShdslEndpointThreshSNRMargin value) has been reached/exceeded for the HDSL2/SHDSL segment endpoint.
Loop Attenuation Threshold Exceeded	indicates that the loop attenuation threshold (as per the hdsl2ShdslEndpointThreshLoopAttenuation value) has been reached/exceeded for the HDSL2/SHDSL segment endpoint.

Clearing the Event Log File

➤ To clear the Event Log file:

1. From the Event Log file, press ‹**C**› to clear all events from the file.

   The following screen appears:

```
Are you sure you want to clear all alarms (Y/N)?
```

2. Press ‹**Y**› to clear or ‹**N**› to return to the Event Log screen.

6.4 Troubleshooting

Use the chart shown in *Table 6-18* to identify and remedy problems in unit operation.

Table 6-18. Troubleshooting Chart

Fault	Probable Cause	Remedial Action
Power LED is off	No power supplied to unit	• Check power source. • Check power cable connected and correctly wired.
Ethernet Link LED is off	• No Ethernet Link detected • Ethernet port in switch and LA-210 are not in the same rate or duplex mode	• Check cable connected and correctly wired. • Check switch and LA-210 Ethernet port configuration (negotiation, rate, duplex mode). • Use Event Log File to check events.
No traffic flow between two units	Configuration or logical layer problems	• Use System Interface Status screen for assistance. All active ports that show Activation–Up, should show Operation–Up. • Use Event Log File to check events. • Check LA-210 configuration and, if necessary, other LA-210 parameters.
Partial Traffic Flow	Timing configuration is not properly set	• Check timing settings.

6.5 Testing the Unit

LA-210 checks network integrity by running ping or trace route tests.

Running a Ping Test

You can ping the remote IP host to check the IP connectivity.

➤ **To ping an IP host:**

1. From the Ping menu (Diagnostics › Ping), configure the following:
   - **Destination IP Address:** IP address of the host that you intend to ping, 0.0.0.0 to 255.255.255.255.
   - **Number of Frames to Send**: Select 0 to send a continuous stream of frames, or 1–50 to send a specified number of frames.

- **Frame Length**: Length of the frame (64–1500).

2. Select **Send Ping** to start sending pings.

   The results appear listed in the lower scrolling message window.

3. Select **Stop Ping** to stop the ping test.

```
                              LA-210
Main Menu > Diagnostics > Ping

1.  Destination IP Address                    0.0.0.0)
2.  Number of Frames to Send [0 - 50]        (0)
3.  Send Ping                                (Yes)
4.  Stop Ping                                ()

ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 6-25. Ping Menu

Tracing the Route

This diagnostic utility traces the route through the network from LA-210 to the destination host.

➤ **To trace a route:**

- From the Trace Route menu (Diagnostics > Trace Route), perform the following:
  - Select **Destination address** and enter the IP address of the host to which you intend to trace the route.
  - Select **Display Trace Route** to start tracing.
  - LA-210 starts tracing the route, displaying the IP addresses of all hop nodes.
  - Select **Stop Trace Route** to stop the tracing.

```
                              LA-210
Main Menu > Diagnostics > Trace Route

1. Destination address       …(0.0.0.0)
2. Display Trace Route
3. Stop Trace Route

ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 6-26. Trace Route Menu

OAM Tests

This diagnostic utility traces the OAM monitoring statistics on selected virtual Ethernet connections (Flows). You may trace the OAM monitoring statistics according to the destination address or the maintenance end point (MEP)`.

➤ **To trace OAM monitoring statistics according to the destination address:**

1. From the OAM Tests menu (Diagnostics › OAM Tests), select **Loopback**.

   The Loopback menu appears as illustrated in *Figure 6-25*.

2. Verify that **Destination Type** is set to **Destination Address**.
3. Define the test parameters according to *Table 6-19*.

```
                              LA-210
Main Menu > Diagnostics > OAM Tests > Loopback

1. Flow ID[1 - 8]                    ... (1)
   Flow Name                         ... (No such Flow)
2. Destination Type                      (Destination Address)
3. Destination Address               ... (00-00-00-00-00-00)
4. Number of LBs to Send[0 - 50]     ... (0)

ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 6-27. Loopback Menu – Destination Address

Table 6-19. Loopback Menu – Destination Address

Parameter	Possible Values	Remarks
Flow ID	1 – 8	The ID of the virtual Ethernet connection.
Flow Name		The name of the virtual Ethernet connection you chose. ***Note**: This parameter is Read Only and cannot be configured.*
Destination Type	Destination Address Remote MEP ID	The destination type for the OAM test **Default: Destination Address**
Destination Address		The MAC address of the destination device
Number of LBs to Send	0 – 50	The number of loobacks. **Default: 0**

➤ **To trace OAM monitoring statistics according to the Remote MEP IDs:**

1. From the OAM Tests menu (Diagnostics > OAM Tests), select **Loopback**.

   The Loopback menu appears as illustrated in .

2. Set **Destination Type** to **Remote MEP ID**.

   Remote MEP parameters appear as illustrated in *Figure 6-26*.

3. Define the test parameters according to *Table 6-20*.

```
                              LA-210
Main Menu > Diagnostics > OAM Tests > Loopback

1. Flow ID[1 - 8]                      ... (1)
   Flow Name                           ... (No such flow)
2. Destination Type                        (Remote MEP ID)
3. Remote MEP ID[1 - 65535]            ... (0)
   Remote MEP Address                  ... (00-00-00-00-00-00)
4. Number of LBs to Send[0 - 50]       ... (0)

ESC-Previous menu; !-Main menu; &-Exit; ?-Help
```

Figure 6-28. Loopback Menu – Remote MEP ID

Table 6-20. Loopback Menu – Remote MEP ID

Parameter	Possible Values	Remarks
Flow ID	1 – 8	The ID of the virtual Ethernet connection.
Flow Name		The name of the virtual Ethernet connection you chose. ***Note**: This parameter is Read Only and cannot be configured.*
Destination Type	Destination Address Remote MEP ID	The destination type for the OAM test **Default: Destination Address**
Remote MEP ID	0 – 65535	ID of the remote maintenance endpoint, terminating the maintenance entity. It must be different from the local MEP ID and unique for the maintenance domain. If set to **0**, no maintenance end point (MEP) is assigned. **Default: 0**
Remote MEP Address		The MAC address of the device assigned as media point at the remote location.
Number of LBs to Send	0 – 50	The number of loobacks. **Default: 0**

6.6 Technical Support

Technical support for this product can be obtained from the local distributor from whom it was purchased.

For further information, please contact the RAD distributor nearest you or one of RAD's offices worldwide. This information can be found at www.rad.com. (Offices – About RAD › Worldwide Offices; Distributors – Where to Buy › End Users)

Appendix A
Pinouts

A.1 Ethernet Connector

The 10/100BaseT Ethernet electrical interface is an 8-pin RJ-45 connector, wired in accordance with *Table A-1*.

Table A-1. 10/100BaseT Ethernet Connector Pinouts

Pin	Function
1	Tx+
2	Tx–
3	Rx+
4, 5	–
6	Rx–
7, 8	–

A.2 SHDSL Connector

The SHDSL electrical interface is an 8-pin RJ-45 connector, wired in accordance with *Table A-2*.

Table A-2. SHDSL Connector Pinouts

Pin	Function
1	NC
2	NC
3	Loop 2
4	Loop 1
5	Loop 1
6	Loop 2
7	NC
8	NC

Note *Do not connect wires to the NC pins.*

A.3 Control Connector

The control terminal interface terminates in a V.24/RS-232 9-pin D-type female DCE connector. *Table A-3* lists the control connector pin assignments.

Table A-3. CONTROL Connector Pinout

Pin	Function
2	Txd (TD)
3	Rxd (RD)
5	Ground (GND)

Appendix B

Boot Manager

This appendix provides a description of the LA-210 boot procedure via an ASCII terminal for downloading software.

The LA-210 software is stored in flash memory in two sections, in the boot sector and in the file system. The boot sector holds a boot program that calls up the rest of the program from the file system.

The file system can hold two compressed copies of the LA-210 code. One copy is called the operating file, and the other is called the backup file. The operating file is the default-executable LA-210 code. The backup file is used whenever the operating file is absent or corrupted.

B.1 Booting LA-210

LA-210 boots up automatically. After powering up, no user intervention is required, except when the user wants to access the file system to modify or update the software or the LA-210 configuration.

Accessing the Boot Manager

The Boot Manager menu is an option that allows the user to perform basic file transfer operations. These operations are all optional.

➤ **To access the Boot Manager menu:**

- Press ‹**Enter**› several times immediately after powering up LA-210.

  The Boot Manager menu is displayed (see *Figure B-1*).

```
LA-210 Boot Version 1.00 (Jan 20 2005)
Boot manager version 7.02 (Jan 20 2005)

0 - Exit Boot-Manager
1 - Dir
2 - Set Active Software Copy
3 - Delete Software Copy
4 - Download an Application by XMODEM
5 - Format flash
6 - Show basic hardware information
7 - Reset board
8 - System Configuration.
9 - Download an Application by TFTP
Press the ESC key to return to the Main Menu.
Select:
```

Figure B-1. Typical Boot Manager Menu

From the Boot Manager menu, you can:

- List all files stored in the flash memory
- Exchange the operating and backup files
- Delete the operating file; the backup file becomes the operating file
- Download a new operating file via XMODEM; the previous operating file is saved as the backup file
- Delete all software and configuration files
- Display the basic hardware information (RAM, ROM size etc)
- Reset the LA-210 board
- Configure the LA-210 IP address, IP mask and default gateway for the consecutive file download via TFTP.

If you choose to exchange or delete a file, you are prompted for confirmation.

B.2 Transferring the Software and Configuration Files

New software releases are distributed as separate files, which are downloaded to LA-210 using the XMODEM protocol or TFTP from the Boot Manager menu. Alternatively, you can download a new software release via TFTP, when the LA-210 management software is already running (Main menu > Utilities > File Transfer).

The TFTP protocol can also be used for uploading configuration files that contain the LA-210 database to the management station. When LA-210 is running, administrators can use this capability to distribute verified configuration files to all other units that use the similar configuration.

Downloading Application Files via XMODEM

Downloading application files using the XMODEM protocol is performed from the Boot Manager menu.

➤ **To download application file via XMODEM:**

1. Configure your ASCII terminal or terminal emulation utility running on your PC to the 115.2 kbps data rate.
2. Access the Boot Manager menu.

   The Boot Manager menu appears (see *Figure B-1*).
3. From the Boot Manager menu, select **Download Files or an Application by XMODEM**.

   LA-210 displays the following message:
   `Select Copy number for download (0)`
4. Select the backup partition by typing its number, **0** or **1**.

   LA-210 responds with the following string:
   `Please start the XMODEM download.`
5. Send the software release file to LA-210 using the XMODEM utility of you terminal application.

   Once the downloading is completed, LA-210 saves the new release as an active partition, the former active partition turns into backup, and the boot sequence continues normally.

   If a failure occurs during the download, the partially downloaded software is erased. In this case, only active software is left in the flash memory.

Downloading Application Files via TFTP

➤ **To download application file via TFTP:**

1. From the Boot Manager menu, select **System Configuration**.
2. Configure the IP parameters of LA-210 (IP address, IP mask and default gateway). These parameters are valid only for the TFTP file transfer via the Boot Manager and can be changed later.
3. Reset LA-210
4. Start a TFTP application.
5. Configure the connection timeout of the TFTP server to be more than 30 seconds to prevent an automatic disconnection during the backup partition deletion (about 25 seconds).
6. Select a local software release file to download.
7. Enter the TFTP server address.
8. Start downloading.

   LA-210 automatically erases the backup partition (it takes about 25 seconds). Once the downloading is completed, LA-210 saves the new release as an active partition, the former active partition turns into backup.

Appendix C

Operation, Administration and Maintenance (OAM)

This appendix describes the Ethernet OAM functionality of LA-210.

C.1 Introduction

Currently LA-210 support pre-standard implementation of Ethernet OAM based on Y.1731 and standard implementation based on Y.1731 and IEEE P802.1ag. The pre-standard implementation is only used for performance measurements when using two RAD units working opposite each other or when working against a RAD that runs an older version of RAD's Ethernet OAM software. This appendix describes the pre-standard implementation. The standard implementation can be found in the standards Y.1731 and IEEE P802.1ag documents.

LA-210 has the following capabilities for providing operation, administration, and maintenance (OAM) in the packet-switched networks:

- Continuity check
- Non-intrusive loopback which used to detect loss of bidirectional continuity
- Performance measurements (per service).

Table C-1 lists the Ethernet OAM-related terms used in the appendix.

Table C-1. Ethernet OAM Terminology

Term	Description
UNI	User Network Interface. The physical demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber
UNI_C	Customer side of a UNI link
UNI_N	Network side of a UNI link
Service frame	An Ethernet frame transmitted across the UNI toward the Service Provider or an Ethernet frame transmitted across the UNI toward the Subscriber.
Flow	Ethernet Virtual Connection : An association of two or more UNIs that limits the exchange of Service Frames to UNIs in the Ethernet Virtual Connection
Point-to-point Flow	Flow connecting exactly two UNIs

Term	Description
Multipoint-to-Multipoint Flow	Flow connecting two or more UNIs
Service Instance / Class of service (CoS)	A set of Service Frames that have a commitment from the Service Provider to receive a particular level of performance
Service Instance Identifier (CoS ID)	Service Frame delivery performance is specified for all Service Frames transported within a flow with a particular Class of Service instance. The Class of Service instance is identified by a Class of Service Identifier associated with each Service Frame (Class of service can be identified by more than one parameter/frame attribute)
MEP	Proactive OAM reference point which is capable to initiate and terminate proactive OAM frames. MEP is also capable to initiate and react to diagnostics OAM frames.
MIP	A provisioned OAM reference point which is capable to respond to diagnostics OAM frames initiated by the MEP.
MEP Service Instance Source	The receiver of OAM frames in each Service Instance
MEP Service Instance Destination	The transmitter of OAM frames in each Service Instance

C.2 Reference Architecture

Figure C-1 illustrates two OAM flows:

- OAM flow originating from the CPE

  The CPE-to-CPE OAM flow is transferred transparently by LA-210 and treated as data.

- OAM flow originating from the LA-210 devices.

  The LA-210 OAM flow runs on a data flow on the same VLAN.
  The LA-210 units terminate the OAM flow and can be referred as a Maintenance Entity (ME). Each device supports up to 8 such MEs. In this case, the LA-210 units act as MEPs (Maintenance End-Points) and not as a MIP (Maintenance Intermediate Points) and all measurements are performed on the UNI_N to UNI_N segment.

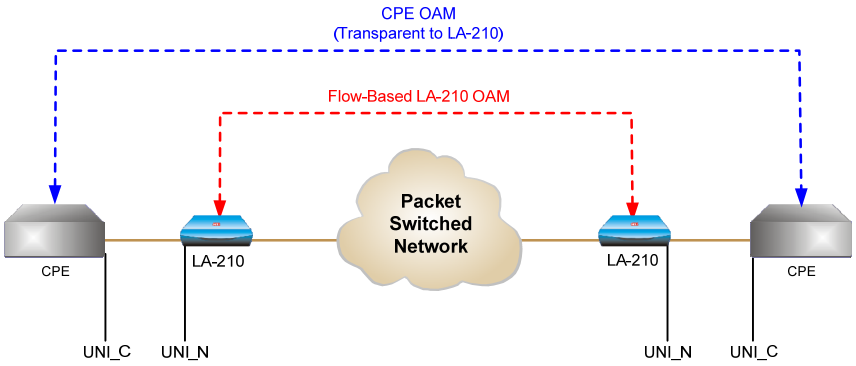


Figure C-1. OAM Architecture

Handling of OAM Levels

UNI_C to UNI_N Direction

In the UNI_C to UNI_N direction LA-210 blocks all OAM messages with OAM level greater than 2. Messages with other OAM levels are passed transparently.

Network Ingress to UNI_N Direction

All OAM messages coming from the network ingress with the ETX MAC address or with the special OAM multicast address are sent to the CPU. All other OAM messages are passed transparently to the user ports as per the respective flow definition.

C.3 OAM Entities

This section describes the OAM entities hierarchy. *Figure C-2* illustrates the relationship between UNI, flow and Service Instance (COS ID), when one or more service instances belong to one flow and one or more flow belong to a UNI. From the OAM perspective, the continuity messages and defects are activated per flow, and the PM is activated per service instance.

Note *A flow can belong only to one UNI in the same LA-210.*

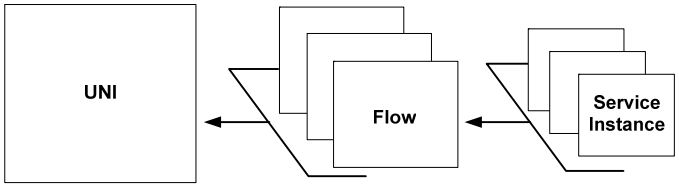


Figure C-2. UNI, Flow and Service Instance (COS ID)

Figure C-3, *Figure C-4* and *Figure C-5* illustrate different combinations of UNIs, flows and service instances. Each UNI contains at least one flow, which contain at least one service instance.

- In the one flow per UNI case (*Figure C-3*), the PM and CC are transmitted once.

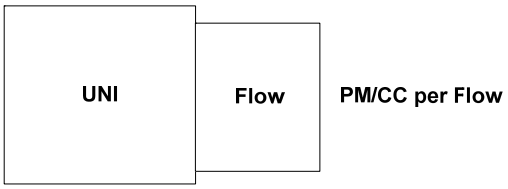


Figure C-3. One Flow per UNI

- In case of multiple flows per UNI (*Figure C-4*), PM and CC are transmitted three times.

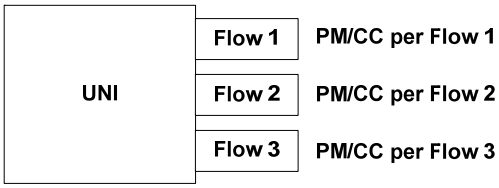


Figure C-4. Multiple Flows per UNI

- In case of one flow and multiple CoS (Service Instances) per UNI (*Figure C-5*), the PM is transmitted three times and the CC – once.

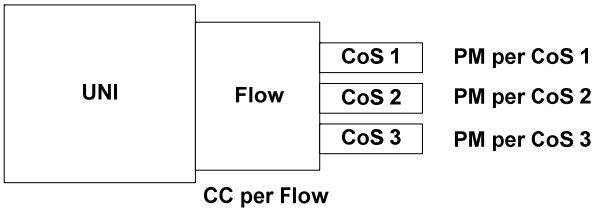


Figure C-5. One Flow and Multiple CoS (Service Instances) per UNI

C.4 OAM Flows

Figure C-6 illustrates a typical OAM traffic flow. The OAM message is transmitted from the source MEP 1 to the destination MEP 2 and the reply is transmitted back The source is also a destination for messages from the other direction.

The OAM interval is one second, so each NTU transmits one request and one reply and receive one request and one reply. Total of four messages are transmitted per second per service instance.

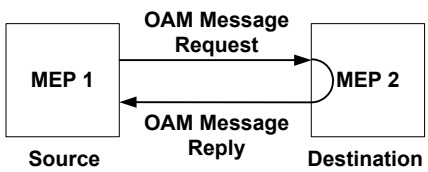


Figure C-6. OAM Flow

OAM Messages Addressing

The OAM defines two modes of addressing, unicast and multicast. Unicast addressing is used for point-to-point connections, while multicast addressing is

used in cases where the MAC address of the destination MEP is not known. Currently LA-210 supports point-to-point flows only.

OAM Message Association

On the receiver side the OAM frame is associated with a flow and a service.

Flow Association

When an OAM frame is associated with a flow, the following steps are performed:

- Request message reception

  When a request message is received, the VLAN is extracted to find the Flow ID. The Flow ID found at the receiver is compared against the Flow ID in the frame. If the IDs are equal, further service association is made. If it is not found, the "Flow ID no match" notification is returned in the reply message.

- Reply message reception

  When a reply message is received, the VLAN is extracted to find the Flow ID. The Flow ID found at the receiver is compared against the Flow ID in the frame. If the IDs are equal, further service association is made. If it is not found, the frame is discarded and connectivity alarm is issued.

Service Association

When an OAM frame is associated with a service, the following steps are performed:

- Request message reception

  The class of service characteristics are extracted from the frame and must be matched to an entry in the flows <-> services table at the receiver. If they are matched, the frame is processed. If not, the service ID is returned with the "Not Found" notification.

- Reply message reception

  The class of service characteristics are extracted from the frame and must be matched to an entry in the flow <-> services table at the receiver. If they are matched, the frame is processed. If not, the frame is discarded.

Ethernet Loopback (ETH-LB)

The ETH-LB can be used to verify connectivity. The ETH-LB is performed by sending a request ETH-LB message to the remote unit and expecting an ETH-LB reply message back to verify connectivity. When the insertion rate of ETH-LB messages is much slower compared to data rate between the flow points, ETH-LB is suitable to perform in-service connectivity verification and to measure round trip delays.

The message is initiated by the local device and runs periodically making it suitable for fault detection.

Unicast ETH-LB request message is sent from a MEP to a specific MEP (remote device). The DA of the request message is a unicast MAC address of destination device. Upon receipt of the request message, the MEP responds with unicast ETH-

LB reply message. The DA of the reply message is a unicast MAC address of requesting device, learned from request message.

Continuity Check (ETH-CC)

Ethernet Continuity Check (ETH-CC) can be used to detect continuity failures across flows between a given pair of edge service point on a flow. Continuity failures are caused by:

- Major failures (link failure, device failure, network path failure etc)
- Minor failures (software failure, memory corruption, incorrect configuration etc).

The ETH-CC signal is generated by one MEP. Upon receipt of the first ETH-CC signal from a sending MEP, the receiving MEP detects continuity with sending MEP and expects to receive further periodic ETH-CC signals. Once the receiving MEP stops receiving periodic ETH-CC signals from sending MEP, it declares continuity failure. The MEP that detects the continuity failure notifies the operator by sending an alarm or a trap.

OAM Procedures

This section discusses the continuity check (CC) and the performance measurement (PM) procedures.

Continuity Check Procedure

The loopback message and the ETH-CC messages are used for continuity check. In case the services are defined and PM collection is enabled, they are also used to carry PM messages. If PM collection is disabled, the messages are used for continuity check only.

If the RX CC mode of the receiver is configured to CC-based, the continuity detection is based on ETH-CC. If the mode is set to LB-based, the continuity detection is based on ETH-LB. If the mode is disabled, the continuity detection is not performed.

ETH-LB Method

The ETH-LB method includes the following elements:

- Unicast ETH-LB transmission

  Unicast ETH-LB request message is transmitted by a MEP (LA-210) every 1 second. The transmitted Transaction Identifier is retained for at least 5 seconds after the unicast ETH-LB signal is transmitted. The Transaction Identifier must be changed for every unicast ETH-LB message, and no Transaction Identifier from the same MEP is allowed to be repeated within 1 minute.

- Unicast ETH-LB reception and reply transmission

  Whenever a valid unicast ETH-LB request message is received by MEP (LA-210), a unicast ETH-LB reply message is generated and transmitted to the requesting MEP. Every field in the unicast ETH-LB request message is copied to the unicast ETH-LB reply message with the following exceptions:

- The source and destination MAC addresses are swapped.
- The OpCode field is vendor-specific oxFE.
- The Flow and MEP ID are processed as follows: if the Flow/MEP ID do not exist in the device, it changes them to No Match" otherwise they are left intact.

- Unicast ETH-LB reply receipt

  When a unicast ETH-LB reply message is received by a MEP (LA-210) diagnostic flow termination function, it examines the TLVs returned in the unicast ETH-LB reply message. The signal is declared invalid if the TLVs do not match those sent in the corresponding unicast ETH-LB request signal, including MEP ID and Flow ID.

- Continuity declarations

  Loss of Continuity and Connectivity Mismatch states are declared by the ETH-LB mechanism.

  - Loss of continuity declaration

    After the source device sends an ETH-LB message a timer is set with a 3.52 second timeout. If the destination device does send reply within the timeout, the source enters the loss of continuity state. Upon reply from the destination, the source resets the timer to 23.5 seconds. Regarding the continuity check message, the source checks only the Flow ID with the MEP ID. When the source enters the loss of continuity state, it adds 24 to Unavailable Seconds counter. The 23.5 second period is calculated as a sliding window.

    Loss of continuity state is cleared after 3.52 seconds with at least 21 reply messages from the destination. In this case the Unavailable Seconds counter decreased by 24.

  - Connectivity mismatch declaration

    If the source Flow ID is not equal to the destination Flow ID as recorded in the reply message for 10 consecutive times, the source enters in to misconnection state.

    Misconnection state is cleared after 10 consecutive reply messages with the correct flow name from the destination.

    The Unavailable counter is maintained by the service according to the number of PM messages that did not receive replies. If a mismatch notification is received to the LB request, the frame is dropped and reply message is not sent. This is why the service becomes unavailable (no reply) in case of mismatch and the unavailable counter is raised.

ETH-CC Method

The ETH-CC method includes the following elements:

- ETH-CC transmission

  Unicast ETH-CC request message is transmitted by a MEP (LA-210) every 1 second. The transmitted Transaction Identifier is retained for at least 5 seconds after the unicast ETH-CC signal is transmitted. The Transaction Identifier must be changed for every Unicast ETH-CC message, and no

Transaction Identifier from the same MEP is allowed to be repeated within 1 minute.

- Unicast ETH-CC reply receipt

  When a unicast ETH-CC message is received by a MEP (LA-210) diagnostic flow termination function, it examines the TLVs returned in the unicast ETH-CC message, and declares the signal invalid if the TLVs do not match those sent in the corresponding exiting MEP ID and Flow ID.

- Continuity declarations

  Loss of Continuity and Connectivity Mismatch states are declared by the ETH-CC mechanism.

  - Loss of continuity declaration

    When the MEP receives the ETH-CC message a timer is set with a 3.5 seconds timeout. If the source does send another message during this period, the destination enters the loss of continuity state. Upon receipt of the ETH-CC message, the destination resets the timer to 3.5 seconds. Regarding the continuity check message, the destination check the Flow ID and the MEP ID. When the destination enters the loss of continuity state, it adds 4 to the Unavailable Seconds counter. The 3.5 second period is calculated as a sliding window.

    Loss of continuity state is cleared after 3.5 seconds with at least 2 messages from the source. In this case the Unavailable Seconds counter is decreased by 4.

  - Connectivity mismatch declaration

    If the source Flow ID is not equal to the destination Flow ID for 10 consecutive times, the destination enters in to misconnection state.

    Misconnection state is cleared after 10 consecutive reply messages with the correct flow name from the source.

    The Unavailable counter is maintained by the service according to the number of PM messages that did not receive replies. If a mismatch notification is received to the LB request, the frame is dropped and reply message is not sent. This is why the service becomes unavailable (no reply) in case of mismatch and the unavailable counter is raised.

Performance Measurement

LA-210 measures performance during 15-minute intervals. It also stores performance history data of nthe last 24 hours (96 intervals). *Table C-2* lists the PM counters supported by LA-210.

Table C-2. PM Counters

Parameter	Description
Frames Above Delay Obj.	Number of frames that exceeded delay objective
Frames Below Delay Obj.	Number of frames below or equal delay objective
Frames Above DV Obj.	Number of frames that exceeded delay variation objective
Frames Below DV Obj.	Number of frames below or equal delay variation objective

Parameter	Description
Frames Transmitted	Total number of OAM frames transmitted in the current interval
Frames Lost	Number of frames lost in the current interval
Unavailable Seconds	Number of seconds during which the service was unavailable in the current interval
Elapsed Time	Time (in seconds) elapsed from beginning of the interval 0–900
Min. RT Delay	Minimum round trip delay (in mseconds) calculated in the interval (or up to elapsed time in current interval)
Avg. RT Delay	Average round trip delay (in mseconds) calculated in the interval (or up to elapsed time in current interval)
Max. RT Delay	Maximum round trip delay (in mseconds) calculated in the interval (or up to elapsed time in current interval)
Avg. DV	Average delay variation (in mseconds) calculated in the interval (or up to elapsed time in current interval)
Max. DV	Maximum delay variation (in mseconds) calculated in the interval (or up to elapsed time in current interval)
OAM Transmitted Frames Counter	Total number of OAM frames transmitted since the service was enabled
OAM Frames Loss Counter	Total number of OAM frames lost since the service was enabled
OAM Frame Loss Ratio	Total number of lost OAM frames divided by total number of transmitted OAM frames since the service was enabled
Elapsed Time	Time (in seconds) elapsed since the service was enabled
Unavailable Seconds	Total number of unavailable seconds since the service was enabled
Unavailability Ratio	Total number of unavailable seconds divided by elapsed time

C.5 RMON Statistics

In addition to the regular statistics collection, LA-210 supports proactive SLA measurements per LA-210 port, as per RMON-based RFC 2819. The device sends reports when one of the available counters (physical layer or OAM) rise above or drop below the set thresholds within the specified sampling period of time. These reports can be sent as SNMP traps to the defined network management stations or be written to the event log.

The following counters can be monitored:

- Dropped Frames
- Undersize Frames
- Oversize Frames
- Fragmented Frames
- Jabbers

- Frame Loss Ratio
- Frames Above Delay
- Frames Above Delay Variation
- Unavailability Ratio.

Index

–A–

AC Power, 2-5
Additional tasks, 4-45
Aging, 1-7
Aging Process
  VLAN-Aware bridge, 1-9
  VLAN–Unaware bridge, 1-11
Application-level status
  displaying, 6-6
Applications, 1-2

–B–

Boot Manager, B-1
Boot sequence, B-1
Booting, B-1
Bridge, 1-7
  Ethernet access, 1-7
  specifications, 1-16
  VLAN Stacking mode, 1-12
  VLAN Stripping mode, 1-12
  VLAN-Aware, 1-8
Bridge features
  VLAN-Unaware
    bridge, 1-11
Bridge port, 4-20
Bridge ports
  configuring, 4-22

–C–

Clock source, 1-6
ConfiguRAD, 1-5, 3-13
  choosing options, 3-14
  configuring access, 4-4
  logging in, 3-13
  menu map, 3-14
  menus
    navigating, 3-14
  web browser requirements, 3-13
configuration
  Radius, 4-6
Configuration, 4-1
Configuring, 4-1
  bridge port, 4-20
  Classifying flows, 4-30
  date, 4-11
  defining flows, 4-29
  device information, 4-1
  Fast Ethernet port, 4-13
  fault propagation, 4-10
  Flows, 4-27
  Flows Intefaces, 4-27
  Internal bridge, 4-17
  IP host parameters, 4-2
  management access, 4-4
  network managers, 4-9
  ports, 4-13
  QoS priorities, 4-23
  SHDSL port, 4-15
  terminal parameters, 4-3
  time, 4-11
  user priorities, 4-23
  VLAN membership, 4-22
Connections
  AC power, 2-5
  DC Power, 2-5
Connectivity tests, 6-24
Control interface
  pinouts, A-2
Control port, 1-16, See Terminal
CoS, 4-33

–D–

Date
  configuring, 4-11
DC Power, 2-5
Description
  functional, 1-7
  physical, 1-6
Device information, 4-1
Diagnostics, 1-15, 1-17, 6-1
  connectivity tests, 6-24
  ping, 6-24
  trace route, 6-25
Downloading application
  via TFTP, B-3

–E–

EFM, 1-1
End-to-end
  statistics, 6-17
Environment
  technichal specifications, 1-18
Equipment
  cable, 2-2
  connectors, 2-2
  hand tools, 2-2
  kits, 2-2
  power cable, 2-2
Equipment for installation, 2-2
Ethernet. See Fast Ethernet
  access, 1-7
  ports, 2-3
Ethernet in the First Mile. See EFM
Ethernet interface, 1-3
  pinouts, A-1

Ethernet port statistics
clearing, 6-9
displaying, 6-8
Ethernet ports, 1-17
Ethernet status, 6-3
Even log file
accessing, 6-21
Event log file
displaying, 6-21
Event Log file, 1-15
clearing, 6-23
displaying, 6-21

–F–

Factory defaults, 4-49
Fast Ethernet port, 4-13
Fault propagation, 1-5
configuring, 4-10
File downloading, B-2
File transfer, 4-48, B-2
Flows, 4-27
classifying, 4-30
defining, 4-29
defining a class of service, 4-33
encapsulating packets, 4-31
interface, 4-27
statistics, 6-17
viewing adding new, 4-36
viewing existing, 4-36
Forwarding, 1-7
Forwarding Process
VLAN-Aware bridge, 1-10
VLAN–Unaware bridge, 1-12

–H–

Host IP, 4-2

–I–

Indicators, 3-1
front panel, 1-17
rear panel, 1-17
Ingress, 1-7
Ingress process, 1-8
admint VLAN tagged frames, 1-9
admit all frames, 1-9
VLAN-Aware bridge, 1-8
VLAN–Unaware bridge, 1-11
Installation, 2-1
connecting to the power, 2-5
equipment, 2-2
Interfaces, 1-7
Control, 1-7
Ethernet, 1-7
pinouts
control, A-2
Ethernet, A-1
SHDSL, A-1
statistics, 6-8
WAN, 1-7
Internal bridge, 4-17
Inventory, 4-45

–L–

Learning, 1-7
Learning Process
VLAN-Aware bridge, 1-9
VLAN–Unaware bridge, 1-11
LEDs, 3-1, 3-2
Line interface, 1-16
Line Interface, 1-1
Login
terminal, 3-10

–M–

Main features, 1-2
Management, 1-5, 1-14
access, 4-4
access, 1-14
access method, 4-4
in-band, 1-14
OOB, 1-14
Management screens
navigating tables, 3-11
Manager List, 4-9
Menu tree, 3-14
Menus
Ping, 5-19
reference, 3-14
Monitoring, 6-1
Event Log file, 6-21
MAC table, 6-6
port statistics, 6-8, 6-9, 6-10, 6-15
port status, 6-3, 6-4, 6-5
radius statistics, 6-20
statistics, 1-16, 6-8
status, 6-1
system messages, 6-21
system status information, 6-1

–N–

Network interface
default settings, 3-2

–O–

OAM, 4-34
statistics, 6-17
Operation, 3-1, 4-10
device level parameters, 4-10
Overview, 1-1

–P–

Package contents, 2-2
Panels
front, 3-1
Password, 4-46
default, 3-10
Physical
technical specifications, 1-18
Physical ports, 4-13
Ping, 6-24
Pinouts, A-1
Ports
connecting, 2-3
Ethernet, 2-3

Power source, 1-17
Powering
  down, 3-17
  up, 3-1
Prerequisites, 2-1
PVID assignment, 1-8

–Q–

Qos
  priorities for traffic queues for 802.1p
    assigning, 4-24
  priorities for traffic queues for DSCP
    assigning, 4-24
  queue profiles, 4-25
QoS
  traffic classification method, 4-23
Quality of Service, 1-4, 1-13, 4-23

–R–

radius
  parameters, 4-7, 4-8
Radius
  configuration, 4-6
Radius statistics
  displaying, 6-20
Required connection media, 2-2
Reset
  device, 4-49
  factory defaults, 4-49
RM-33-2, 2-2

–S–

Screen
  help, 3-12
Security, 1-5
Setup, 2-1
SHDSL interface, 1-3
  pinouts, A-1
SHDSL line status, 6-4
SHDSL PCS line statistics
  displaying, 6-10
SHDSL PCS port statistics
  displaying, 6-10
SHDSL PCS status, 6-5
SHDSL PME
  statistics
    15 minute interval, 6-11
    accumulated data, 6-14
    current interval, 6-12
    day interval, 6-13
SHDSL port, 4-15
SHDSL port statistics, 6-10
  clearing, 6-15
Site requirements, 2-1
SNMP
  configuring access, 4-4
Software
  downloading, B-1
  files, B-1
  in flash memory, B-1
  new releases, 4-48
  updates, 4-48, B-2
  versions, 4-48
Specifications
  bridge, 1-16
Statistics, 1-6, 1-15, 6-8
  end-to-end, 6-17
  OAM, 6-17
System messages, 6-21

–T–

Technical specifications, 1-16
Technical support, 6-28
Telnet, 4-4
Terminal
  baud rate, 4-3
  choosing options, 3-10
  logging in, 3-10
  login, 3-10
  parameters, 4-3
  starting control session, 3-9
  working with, 3-9
TFTP, B-2, B-3
  download, B-3
Time
  configuring, 4-11
Timing, 1-6, 1-17
Trace route, 6-25
Transmission, 1-7
Transmission Process
  VLAN-Aware bridge, 1-10
  VLAN–Unaware bridge, 1-12
Troubleshooting, 1-15, 6-1, 6-24

–U–

Unit enclosure, 1-1
User interface
  default settings, 3-2
User name, 4-46
Utilities
  factory defaults, 4-49
  file transfer, 4-48
  reset device, 4-49

–V–

Versions, 1-1
VLAN membership, 4-22
VLAN-Aware mode, 1-8
VLAN-based management scheme, 1-14
VLAN–Unaware mode, 1-11

–X–

XMODEM, B-3

AC/DC Adapter (AD) Plug

for DC Power Supply Connection

Note *Ignore this supplement if the unit is AC-powered.*

Certain units are equipped with a wide-range AC/DC power supply. These units are equipped with a standard AC-type 3-prong power input connector located on the unit rear panel. This power input connector can be used for both AC and DC voltage inputs.

For DC operation, a compatible straight or 90-degree AC/DC Adapter (AD) plug for attaching to your DC power supply cable is supplied with your RAD product (see *Figure 1* and *Figure 2*).

Connect the wires of your DC power supply cable to the AD plug, according to the voltage polarity and assembly instructions provided on *page 2*.

Figure 1. Straight AD Plug

Figure 2. 90-Degree AD Plug

Caution

Prepare all connections to the AD plug **before** inserting it into the unit's power connector.

➤ **To prepare the AD plug and connect it to the DC power supply cable:**

1. Loosen the cover screw on the bottom of the AD plug to open it (see *Figure 3*).
2. Run your DC power supply cable through the removable cable guard and through the open cable clamp.
3. Place each DC wire lead into the appropriate AD plug wire terminal according to the voltage polarity mapping shown. Afterwards, tighten the terminal screws closely.
4. Fit the cable guard in its slot and then close the clamp over the cable. Tighten the clamp screws to secure the cable.
5. Reassemble the two halves of the AD plug and tighten the cover screw.
6. Connect the assembled power supply cable to the unit.

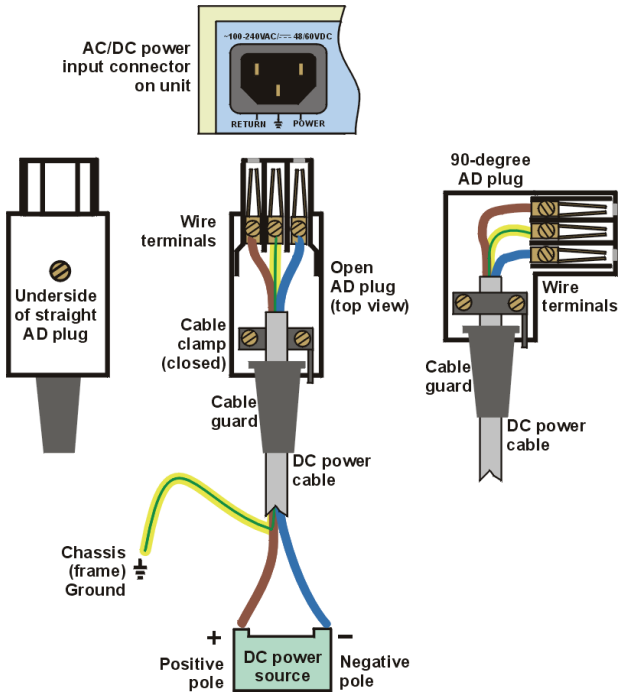
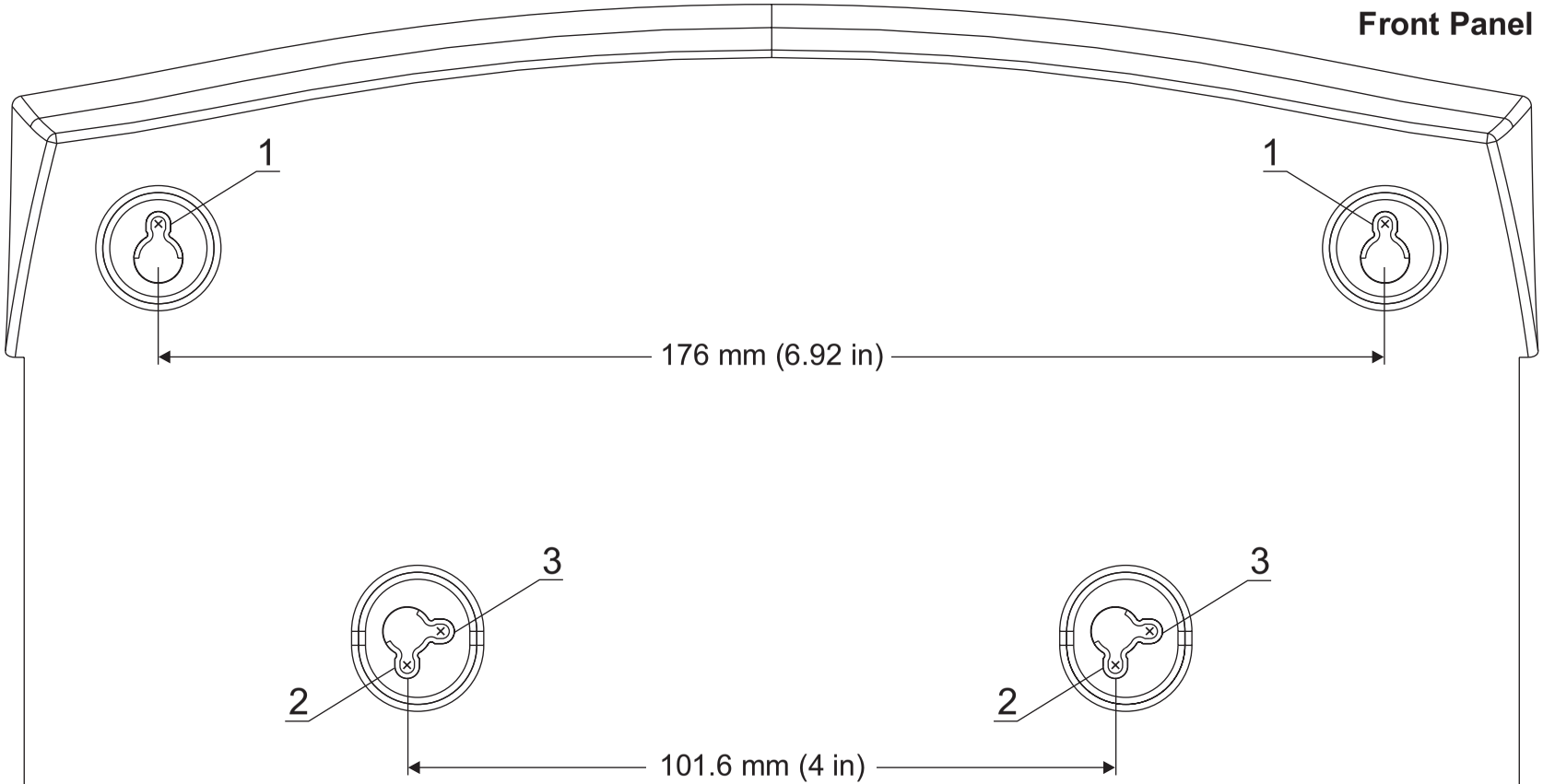


Figure 3. AD Plug Details

Warning

- **Reversing the wire voltage polarity will not cause damage to the unit, but the internal protection fuse will not function.**
- **Always connect a ground wire to the AD plug's chassis (frame) ground terminal. Connecting the unit without a protective ground, or interrupting the grounding (for example, by using an extension power cord without a grounding conductor) can damage the unit or the equipment connected to it!**
- **The AD adapter is not intended for field wiring.**

Supplement
Drilling Template for Wall Installation



This panel is drawn to scale.
To drill the holes for a wall installation, tear this page out of the manual or print it on letter-size paper (8.5"x11.0") and hold it against the wall.

LEDs facing up - drill at **1**.
LEDs facing down - drill at **2**.
LEDs facing left - drill at **3**.

RAD data communications
Innovative Access Solutions

24 Raoul Wallenberg Street, Tel Aviv 69719, Israel
Tel: +972-3-6458181, Fax +972-3-6483331, +972-3-6498250
E-mail: erika_y@rad.com, Web site: http://www.rad.com

Customer Response Form

RAD Data Communications would like your help in improving its product documentation. Please complete and return this form by mail or by fax or send us an e-mail with your comments.

Thank you for your assistance!

Manual Name: LA-210 Ver. 1.5

Publication Number: 504-200-08/08

Please grade the manual according to the following factors:

	Excellent	*Good*	*Fair*	*Poor*	*Very Poor*
Installation instructions	❒	❒	❒	❒	❒
Operating instructions	❒	❒	❒	❒	❒
Manual organization	❒	❒	❒	❒	❒
Illustrations	❒	❒	❒	❒	❒
The manual as a whole	❒	❒	❒	❒	❒

What did you like about the manual?

_____

_____

_____

_____

Error Report

Type of error(s) or problem(s):

- ❒ Incompatibility with product
- ❒ Difficulty in understanding text
- ❒ Regulatory information (Safety, Compliance, Warnings, etc.)
- ❒ Difficulty in finding needed information
- ❒ Missing information
- ❒ Illogical flow of information
- ❒ Style (spelling, grammar, references, etc.)
- ❒ Appearance
- ❒ Other _____

Please list the exact page numbers with the error(s), detail the errors you found (information missing, unclear or inadequately explained, etc.) and attach the page to your fax, if necessary.

_____

_____

_____

_____

Please add any comments or suggestions you may have.

_____

_____

_____

You are:

- ❒ Distributor
- ❒ End user
- ❒ VAR
- ❒ Other

Who is your distributor? _____

Your name and company: _____

Job title: _____

Address: _____

Direct telephone number and extension: _____

Fax number: _____

E-mail: _____

Publication No. 504-200-08/08

International Headquarters

24 Raoul Wallenberg Street
Tel Aviv 69719, Israel
Tel. 972-3-6458181
Fax 972-3-6498250, 6474436
E-mail market@rad.com

North America Headquarters

900 Corporate Drive
Mahwah, NJ 07430, USA
Tel. 201-5291100
Toll free 1-800-4447234
Fax 201-5295777
E-mail market@radusa.com

www.rad.com

RAD
data communications
The Access Company